Enabling Technology to Advance Health-Protecting Individual Rights-Are We Walking the Talk?

Crystal Sharp and Femida Gwadry-Sridhar

I-THINK Research, Lawson Health Research Institute, 268 Grosvenor St, FB-112, London, ON N6A 4V2 Canada
crystal.sharp@lawsonresearch.com

Abstract. The evolving structure and business of health care services and delivery need the functionality and capability offered by electronic health record (EHR) systems. By electronically diffusing the traditional patient record, however, this new model blurs the long-established medical data home, raising concerns about data ownership, confidentiality, access and individual rights. In 2008 the Lawson Health Research Institute began the process of instituting a robust health informatics and collaborative research infrastructure, now known as I-THINK Research. As data are migrated to the platform and policies are developed, we are forced to confront the complexity of issues around protection of individual rights. The paper presents, in a broader context, the main issues surrounding the privacy debate and the need for education, accountability and new legislation to help define and protect individual rights as new e-health business models emerge.

Keywords: eHealth, electronic health records, consent, Google Health, Microsoft Vault, personal health records, privacy, confidentiality.

1 Introduction

In 2008 the Lawson Health Research Institute (the research institute for the London Health Sciences Centre and St. Joseph's Health Care in London, Ontario, Canada) began the process of instituting a robust health informatics and collaborative research infrastructure, now known as I-THINK Research[1]. Our ethos is that a secure and common platform for rich clinical, biomarker, genomic and imaging data, that otherwise exists in silos, will enable collaborative research yielding deeper insight into disease etiology and better care strategies for patients. As data are migrated to the platform and policies are developed, we are forced to confront the complexity of issues around protection of individual rights. This paper discusses some of the complexities but in a broader context because as health researchers, practitioners and consumers we are all affected by rapidly evolving use of health technology, new business models, privacy legislation and definitions of ownership, sharing and management of personal data.

It is a surprising fact, given the rapid adoption of computerization in business and personal use, that doctors in most parts of the world still work mainly with pen and paper[2]. Even in an advanced industrialized economy like the USA, a recent study

P. Kostkova (Ed.): eHealth 2009, LNICST 27, pp. 51–61, 2010.

found that only 1.5% of acute care hospitals in the American Medical Association had a comprehensive electronic-records system (present in all clinical units), an additional 7.6% had a basic system (present in at least one clinical unit); and computerized provider-order entry for medications were implemented in only 17% of hospitals[3]. The 2009 American Recovery and Reinvestment Act has recently allocated up to $20 billion to implement clinical information systems, anticipating use of electronic health information for each person in the United States by 2014[2]. Given the current low levels of adoption of electronic health records in U.S, however, the combination of financial support, interoperability, and training of technical support staff needed to spur adoption of e-health will be considerable[3],[4]. Public policy challenges of implementation will require improvements to existing law, new rules for entities outside the traditional health care sector, a more nuanced approach to the role of consent, and stronger enforcement mechanisms[5]. With rare exception, however, national efforts to advance health information technology have not adequately addressed privacy[5]. The debate about rights to privacy has often seemed too polarized to resolve, grid locking initiatives to promote health information technology. It will be interesting to see how this initiative unfolds.

This paper will present the main issues surrounding the privacy debate in context of the potential of e-health to improve health care, the difficulties in defining ownership of data in a networked world, and the need for education, accountability and new legislation to help define and protect individual rights as new e-health business models emerge.

2 Potential of E-Health

The evolving structure and business of health care services and delivery need the functionality and capability offered by electronic health record (EHR)systems, which offer the potential to[6]: facilitate accurate and efficient flow of patient medical and billing information between organizationally and geographically distinct providers; to enable utilization review; to encourage patient-centred care, by giving patients access to information in their records, particularly when they have fragmented or episodic relationships with multiple providers; and to give providers transparent access to other occasions of treatment, particularly pharmacotherapy. Both patients and regulators want increasing amounts of data regarding errors or near misses and outcomes in populations—data that is difficult to generate without sophisticated data coding and nearly impossible to analyze without complex, comprehensive database systems.

By electronically diffusing the traditional patient record, however, this new model blurs the long-established medical data home, raising concerns about data ownership, confidentiality, access and individual rights. Since electronic health records offer the potential for high-quality, interactive and innovative patient-centred care, it is imperative that such issues are resolved if their full potential is to be realized[7].

3 Difficulty in Defining Ownership of Data

Networked ICT applications in energy, transportation, health and digital libraries, critical to the well-being of humankind, are currently being developed and delivered

via the internet, widening social, economic, and productivity boundaries and creating new value chains[8]. E-health infrastructure upkeep challenges involve high-capacity storage, secure systems, and connectivity for different devices requiring high bandwidth, both wired and wireless. In addition to the hospitals, the care providers, consumers, researchers, insurers and businesses that cater to the needs of healthcare delivery, there are pharmaceutical companies, health systems vendors, medical device producers and data brokers. EHR systems are becoming more and more sophisticated and nowadays include numerous applications, which are not only accessed by medical professionals, but also by accounting and administrative personnel. This could represent a problem concerning basic rights such as privacy and confidentiality. By some views, granting access to an EHR should be dependent upon the owner of the record to define who is allowed to access. But who owns medical information – the one who gives care, receives care, pays for care?[9]. Ownership of paper records was never much in doubt. Clinicians and insurers own the tangible vessels in which they store patients' medical information. But now that digitizing information frees it from particular storage media, confusion reigns. By some views the rights of ownership should belong to the patient[9;10].

Determining ownership of health information is not straightforward and modern health information systems elevate issues of ownership. Health information data may carry personal property rights, with numerous stakeholders making cognizable claims to ownership. The rights to a health information system involve the ascertainment of intellectual property. Both types of property rights - personal and intellectual - are immensely valuable and thus the definition of ownership is important[11],[12]. Many of the legal questions that arise relate to the formation of the information industry. Others, including some of the most difficult-to-resolve issues, involve complex balancing questions. Who should have access to certain types of information? Should industry members enjoy protections against certain types of liability for conduct that may become more evident as the volume of information expands? In other words, should the law recognize certain privileges, “safety zones,” and “safe harbors,” in exchange for the creation, collection, sharing, and use of certain valued information, and if so, what conditions should be placed on sanctioned activities? Finally, are there extreme cases in which the government should compel, rather than merely incentivize and encourage, the creation and production of certain information?[11].

3.1 The Complexities of "Privacy" in a Networked World

Patient concerns about the privacy, confidentiality and security of their health data are legitimate, as disclosure about existing health conditions may affect an individual's employment, ability to get and maintain health coverage without having to pay a high premium. Policy considerations to safeguard privacy amount to balancing individual privacy considerations against the accessibility of health information; delineating the required and permissible purposes for which vast new amounts of health information can be collected, stored, transmitted, used and disclosed; and negotiating the regulatory boundaries of new technologies[11;13].

The effective coordination of health care relies on communication of confidential information about consumers between different health and community care services. The legal and ethical issues involve consent and its alternatives, the handling of identifiability. Matching and combining data from multiple databases, especially at

the individual level, is a powerful tool made possible by the availability of high performance computational power and rich databases. Data linking raises a number of issues. If the data are of sufficient richness to enable identification of individuals simply by adding the various factors such as education, profession, marital status etc. together to reach an almost certain conclusion with regard to the identity of the person, then this is a direct violation of privacy and data protection legislation. Linked-up material does amount to a fuller description than the bits unlinked, and thus may present higher potential for abuse[14-17]. And in the case that the component data are not identified, interlinking them may provide more cues and decrease the difficulty of re-identifying the subjects by deduction. Whether some degree of linkage may be "too much" relative to the benefits and safeguards has to be judged in context[17]. Mobile sensor technologies that gather data ubiquitously and unobtrusively present a whole host of new security and privacy concerns[18].

Distinguishing between the unique needs of information-based research, which uses medical records or stored biological samples, and interventional clinical research, which involves people who participate in experimental treatment, the Institute of Medicine, HIPAA committee, recommends extending the Common Rule (a set of federal regulations for research involving human subjects that requires a review of proposed research by an Institutional Review Board (IRB), the informed consent of research subjects, and institutional assurances of compliance with the regulations) to apply to all interventional research, regardless of funding source[19]. However, Research and Ethics Boards typically do not have the necessary expertise to assess electronic health privacy[20] and this can be a problem.

3.2 Privacy Legislation

The law itself can both advance change and impede it – this is particularly evident in health care. Legal complexities arise as a function of policymakers' efforts to balance the rights of patients and their expectations of privacy; the autonomy and authority of health professionals; market-based economies dominated by the buying and selling of health care; and the delicate balance of jurisdictional powers over health care quality, financing and accountability. No aspect of health care offers a better example of the challenges inherent in balancing these interests than the collection, management, disclosure and reporting of health information [11].

Privacy laws (the Canadian Personal Information Protection and Electronic Documents Act [PIPEDA], US Health Insurance Portability and Accountability Act [HIPAA], and European Union Data Privacy Directive, for example) generally define personal information as *identifiable* information *about* and individual and require that individual's consent before such personal information can be collected, used or disclosed, in the absence of some applicable exception[16].

The concept of informed consent itself is fraught with complications. For instance it is debatable whether a child or a mentally incapacitated individual is adequately informed to be able to consent. Research that is based on retrospectively collected records may never be allowed to commence if subjects cannot be located for their consent. Researchers have legitimate concerns about completeness and validity in sampling and systematic bias in research results if potential research subjects can opt out[21].

The two poles in the consent argument represent a tradeoff between high coverage of the population, where records can be uploaded without explicit consent, and the

opposite situation where explicit consent must be obtained for every record uploaded. As mentioned by Greenhalgh et al (2008), shared electronic record programmes in Scotland (emergency care summary), Wales (individual health record), and France (dossier médical personnel) have to some extent squared this circle by combining "implied consent to upload" with "explicit consent to view" at the point of care, although they have not been without controversy [22].

Although de-identification is a crucial protective strategy in privacy legislation, some entities are not covered under existing privacy legislation. For example, in Canada prescription data is routinely sold or transferred to commercial data brokers who may process the data and re-sell it to pharmaceutical companies in the form of prescribing patterns or practices[15;16;23]. Thus potential patient identifiers and physician-linked prescription data "stream from pharmacy computers via commercial compilers to pharmaceutical companies" without the informed consent of patients or of physicians[23].

Reversible anonymisation, or key-coding, which maintains a connection between substantive data and personal identifiers but does not allow researchers to know the identifiers, could serve both privacy and research well[17]. Properly anonymised data are not "personal," so their processing is not generally regulated by data protection legislation. But anonymisation has its difficulties – because identifiability is a continuum and anonymisation is rarely absolute, and because there can be many reasons for retaining the potential to re-identify data[17]

4 New Business Models – Need for Education, Accountability and New Legislation

4.1 Personalized Medicine

Biobanks (repositories of tissue and DNA samples) yield data that can be linked to personal medical information and test results which in combination can provide insights into disease progression that tissue samples or medical records alone cannot. Drug companies and medical researchers can, for example, pick out samples from people with a particular disease and determine its associated genetic variations to aid drug discovery. Public-health officials and epidemiologists can identify disease patterns in subpopulations and ethnic groups far more quickly than has been possible in the past. Disease-specific biobanks have potential to accelerate research into disorders such as AIDS and breast cancer[24].

In 2005 Britain and Norway announced a plan to co-operate on biobank-based research into the causes of attention-deficit hyperactivity disorder (ADHD), autism, schizophrenia and diabetes. Norway was collecting blood samples and health data from 200,000 citizens and from 100,000 pregnant women. Britain's project, UK Biobank, began gathering blood and urine samples and confidential lifestyle data from 500,000 volunteers aged 40-69, in an attempt to untangle the genetic and environmental causes of heart disease, Alzheimer's, diabetes and cancer. Participants will provide new samples and data for up to 30 years, allowing the development and course of different diseases to be tracked. Similarly, the Karolinska Institute in Stockholm which runs one of the world's oldest university-based biobanks is following 500,000 Swedes for 30 years to gain new insights into depression, cancer

and heart disease. Other national biobank projects include the Estonian Genome Project, Singapore Tissue Network, Mexico's INMEGEN, and Quebec's CARTaGENE. Various university medical schools around the world have been collecting biological samples and clinical data as a matter of routine. These resources, if shared, could now turn out to be extremely valuable for disease discovery[24].

Maintenance of patient confidentiality is a major challenge in a networked environment, because the combination of clinical data and personal data and the place of research can be enough to reveal a research participant's identity[25;26]. Britain's UK Biobank, for example, encrypts the identity of donors, so that only selected users are able to link samples and data to particular individuals. Total anonymity, however, raises problems of its own: it precludes the possibility of informing donors or their relatives if donated material reveals them to be at risk from a specific disease[24].

If a risk of identification remains, patients should be asked for consent to data sharing as well as consent to taking part in the research. The question of confidentiality is bound up with another conundrum: who is going to pay for data storage and maintenance in health grids and biobanks? The answer is unclear. One approach would be to make information freely available to academic and government researchers, but to charge drug companies and other commercial interests which stand to profit from their use of the data. That could make biobanks self-sustaining, or even profitable; it has even been suggested that donors should be given a share of the proceeds. Advances in data-mining technologies and a growing interest in the notion of "personalised" medicine have spurred a growing realisation, in both the health-care and information-technology sectors, that biobanking could be very lucrative[24]. Purists insist that biobanks should remain strictly non-commercial entities. The Genome Institute of Singapore forbids any commercialisation of its biobank data, for example, though so far it is the exception to the rule[24].

4.2 Personal Health Records and Personal Medical Monitoring

Google Health, released in May 2008, and Microsoft HealthVault, launched in October 2007, allow consumers to store and manage their personal medical data online. Users are now able to gather information from doctors, hospitals, and testing laboratories and share it with new medical providers, making it easier to coordinate care for complicated conditions and spot potential drug interactions or other problems. Both Google and Microsoft also offer links to third-party services that provide medication reminders and programs that track users' blood-pressure and glucose readings over time. What Google and Microsoft promise to do with electronic records is also a radical departure, both conceptually and in practice. Currently, patients who have electronic access generally use portals maintained by doctors or health-care systems. Typically, patients can view information such as prescriptions, lab results, and diagnoses; sometimes they can e-mail doctors or make appointments online. In most cases, though, patients do not control their own data, so they cannot transfer it electronically to a different health-care provider or plug it in to third-party applications[27]. With HealthVault and Google Health, however, consumers have fundamental ownership of their medical data, much as they do with financial records. As more health-care providers begin participating, it will be easy for patients to share CT scans, x-rays, and lab results with new doctors[27].

Home medical monitors, such as those for blood pressure, have become a common presence in personal health-care. Wireless technologies and web portals offer new ways to track and store the information gathered by such monitors online, which can make it easier for people to review and share test results. Microsoft HealthVault offers options for tracking health measures at home. Data from these devices can be uploaded manually or automatically via wireless sensors directly into a patient's HealthVault record, where users can then create a handy graph of their blood pressure, weight, blood sugar, or other data, and share it with their doctors or family members[28]. The Mayo Clinic recently launched a free software program, available to anyone, that piggybacks on HealthVault, integrating health history and data from medical monitors and providing reminders about vaccinations and other preventative measures. The Cleveland Clinic started a pilot program using HealthVault in conjunction with different devices to manage three chronic conditions, including diabetes, heart failure, and hypertension. Scientists will track how effective the system is at changing both treatment and patient outcomes. Systems like these enable researchers to gather information in near real time and to act on the results of that information in a more continuous fashion [28]. In the long term, HealthVault is expected to function more as a database for storing data, while third-party applications can help patients organize and act on it[28].

Currently, if you are a Google account holder, you can set up access to Google Health and enter your own medical information and even search your prescription history with a few big pharmacies. In May 2008, Beth Israel Deaconess Hospital joined the Cleveland Clinic to become Google's first partners in the new service, along with and a handful of pharmacies, labs, and other health businesses. If Google Health succeeds at Beth Israel Deaconess, this may forecast whether patients are willing to trust their health information to large personal health record (PHR) providers, and it may hint at how Google Health and similar services might impact medical care in the future[29]. Dr. John Halamka, chief information officer at Beth Israel Deaconess, Chair of the national Health Information Technology Standards Panel, and member of Google Health's advisory council, is a strong believer that patients should be the stewards of their own medical data"[29]. But it is not clear that this view would be universally shared by the medical profession and other important stakeholders.

4.3 Need to Provide Education and Technical Assistance for Consumers

A 2009 study using observational and narrative data to examine the acceptability, adoption and use of personally controlled health records found low levels of familiarity with PCHRs along with high expectations of the capabilities of nascent systems –a potentially problematic pairing[30]. Perceived value for PCHRs was highest around abilities to co-locate, view, update and share health information with providers. Expectations were lowest for opportunities to participate in research. Early adopters perceived that PCHR benefits outweighed perceived risks, including those related to inadvertent or intentional information disclosure. Endorsement of a dynamic platform model PCHR was evidenced by preferences for embedded searching, linking, and messaging capabilities in PCHRs; by high expectations for within-system tailored communications; and by expectation of linkages between self-report and clinical data. The author advocated educational and technical assistance for lay users and providers

as critical to meeting challenges of access to PCHRs (especially among older cohorts); workflow demands and resistance to change among providers; health and technology literacy; clarification of boundaries and responsibility for ensuring accuracy and integrity of health information across distributed data systems; and improving understanding of confidentiality and privacy risks[30].

4.4 Need for Methods to Validate and to Ensure Accountability

Today, many journals are asking authors to include a data sharing statement at the end of each original research article. The statement is required to explain which additional data – if any – are available, to whom, and how. The data can range from additional explanatory material to the complete dataset. Those allowed access to the data might be restricted to fellow researchers only or could include everyone. Data could be available only on request, accessible online with a password, or openly accessible to all on the web with a link. Sharing could allow other researchers –and perhaps scientists, clinicians, and patients, access to raw numbers, analyses, facts, ideas, and images that do not make it into published articles and registries[31]. Potential benefits include quicker scientific discovery and learning, better understanding of research methods and results, more transparency about the quality of research, and greater ability to confirm or refute research through replication. However, such sharing also raises important questions about who owns the data[25] who gives permission to release the data (including funders, research participants, owners of the intellectual property, and copyright holders), where and how the data should be stored (in electronic repositories managed locally, nationally, or internationally; or in subject specific databases), how the data should be stored and managed and made compatible across repositories, how the data should be accessed and mined, who should have access and when, and what limits may be needed to prevent misuse and mishandling of data[31].

4.5 Need for Legislation That Covers All Entities

Existing health data privacy legislation (like HIPAA and PIPEDA) does not cover entities like Google Health and Microsoft Healthvault as they are not healthcare provider organizations. Dr. Halamka, CIO Beth Israel Hospital, a strong supporter of PCHRs, is of the opinion that since Google Health and Microsoft Vault monetize these sites by attracting search traffic, they would be highly motivated to build secure and trustworthy systems. However, there certainly seems to be a need for a privacy protection framework that can be applied to all PCHR products - those tethered to an EHR, those offered by a payer, those sponsored by an employer or those created by third party vendor ensures that consumers have a rubric to evaluate these products[32].

5 Conclusion -- Enabling Technology to Advance Health - Protecting Individual Rights - Are We Walking the Talk?

A cross sectional study in New Zealand examining the public's perception of the security of electronic systems concluded that for the EHR to be fully integrating in the

health sector, there are two main issues that need to be addressed: the security of the EHR system has to be of the highest level and be constantly monitored and updated; and the involvement of the health consumer in the ownership and maintenance of their health record needs to be more proactive. The results from this study indicated that the consumer is ready to accept the transition as long as one could be assured of the security of the system[33].

Within the rapidly changing internet environment, the playing field is indeed global, raising questions about the role of government. In a discussion during the ICT 2008 conference in Lyon, France, the consensus was that government's role in this environment should not be to establish the "grand design"; but to build confidence in the system so that a user asking the following questions can be reassured: "Is my money safe? Is my data secure and being used for the purpose for which it was collected? Is my privacy protected?"[8]. The future of the Internet must be planned and pursued by considering its circular interaction with social and physical-world processes. With all the complexities presented in the networked environment, perhaps control of privacy should be shifted to consumers, allowing them to control the "privacy dial," since we all have varying levels of comfort with openness. Rather than have blanket rules for privacy protection, consumers can be given the tools to set the privacy dial to their level of comfort.

The good news is that the issues presented above are being addressed and debated. Rand Europe has recently reviewed and provided recommendations for addressing limitations in the existing European Data Protection Directive[34] as has the Data Protection Working Party[35]. Led and operated by the Markle Foundation, Connecting for Health is a public-private collaborative that includes representatives from over 100 organizations, comprising a diverse group of health care stakeholders. Connecting for Health has developed a Common Framework for Networked Personal Health Information to address the key challenges. The framework proposes a set of practices that, when taken together, encourage appropriate handling of personal health information as it flows to and from personal health records and similar applications or supporting services[36].

These are steps in the right direction. However, the complexity of technological, societal, economic, stakeholder, individual and political issues in the privacy debate make enforcement of rules extremely difficult, if not impossible. The public sector has a role in encouraging education frameworks that develop innovation and management excellence and in providing a supportive environment for entrepreneurial activity that promotes knowledge transfer and research uptake[8]. Patient-controlled health records offer one potential solution to many of the problems encountered in creating institution-based longitudinal medical records. No matter which path is taken, however, clear but adaptable laws are needed so that stakeholders can assign economic value to the access, control, and use of the medical information contained in electronic health record networks[9]. Until then we will have to be watchful that, at least in our own spheres of operation, we achieve a reasonable balance in encouraging research that can improve health while respecting individual rights.

References

[1] Mann, R., Gwadry-Sridhar, F., Bowman, S., Soer, J.: How to Develop a Common Platform to Enable Interdisciplinary Research. International Journal of Technology, Knowledge and Society 5, 21–38 (2009)

[2] Steinbrook, R.: Personally Controlled Online Health Data – The Next Big Thing in Medical Care? N. Engl. J. Med. 358, 1653–1656 (2008)

[3] Jha, A.K., DesRoches, C.M., Campbell, E.G., Donelan, K., Rao, S.R., Ferris, T.G., Shields, A., Rosenbaum, S., Blumenthal, D.: Use of electronic health records in U.S. hospitals. N. Engl. J. Med. 360, 1628–1638 (2009)

[4] Economist, Medine goes digital: A special report on healthcare and technology. Economist, 1–16 (2009)

[5] McGraw, D., Dempsey, J.X., Harris, L., Goldman, J.: Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange. Health Aff. 28, 416–427 (2009)

[6] Lang, R.D.: Blurring the lines: who owns the medical data home? J. Healthc. Inf. Manag. 22, 2–4 (2008)

[7] Gunter, T.D., Terry, N.P.: The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions. J. Med. Internet. Res. 7, e3 (2005)

[8] Sharp, C.: Conference Report: ICT 2008 - I's to the Future: Invention, Innovation, Impact. Online 33[March/April 2], pp. 22–25. Information Today, Inc. (2009)

[9] Hall, M.A., Schulman, K.A.: Ownership of Medical Information. JAMA 301, 1282–1284 (2009)

[10] Falcao-Reis, F., Costa-Pereira, A., Correia, M.E.: Access and privacy rights using web security standards to increase patient empowerment. Stud. Health Technol. Inform. 137, 275–285 (2008)

[11] Rosenbaum, S., Painter, M.: Assessing Legal Implications of Using Health Data to Improve Health Care Quality and Eliminate Health Care Disparities. The Robert Wood Johnson Foundation (2005)

[12] Bluml, B.M., Crooks, G.M.: Designing solutions for securing patient privacy–meeting the demands of health care in the 21st century. J. Am. Pharm. Assoc. (Wash.) 39, 402–407 (1999)

[13] Conn, J.: Data encryption just one option under security law. Modern Healthcare (2009)

[14] Kelman, C., Bass, A., Holman, C.: Research use of linked health data - a best practice protocol. Australian and New Zealand Journal of Public Health 26, 251–255 (2002)

[15] El Emam, K., Kosseim, P.: Privacy Interests in Prescription Data, Part 2. IEEE Security & Privacy, 75–78 (2009)

[16] Kosseim, P., El Emam, K.: Privacy Interests in Prescription Data, Part 1. IEEE Security & Privacy 72 (2009)

[17] Lowrance, W.W.: Learning from experience: privacy and the secondary use of data in health research. J. Biolaw. Bus. 6, 30–60 (2003)

[18] Nixon, P., Wagealla, W., English, C., Terzis, S.: Security, privacy and trust issues in smart environments, Glasgow, Scotland, The Global and Pervasive Computing Group, Department of Computer and Information Sciences, University of Stathclyde (2009); 5-18-0090

[19] Committee on Health Research and the Privacy of Health Information. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research: Report Brief, Washington DC, Institute of Medicine (2009)

[20] Lysyk, M., El Emam, K., Lucock, C., Power, M., Willison, D.: Privacy Guidelines Workshop Report, Ottawa, Canada (2006) 7-6-0090
[21] Sharp, C.: Electronic Health Information: A boon and a curse! The Free Pint, Newsletter (2001); 7-6-0090
[22] Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Mohammad, Y., Russell, J.: Introduction of shared electronic records: multi-site case study using diffusion of innovation theory. BMJ 337, a1786 (2008)
[23] Zoutman, D.E., Ford, B.D., Bassili, A.R.: The confidentiality of patient and physician information in pharmacy prescription records. CMAJ 170, 815–816 (2004)
[24] Economist. Medicine's new central bankers. Economist (December 8, 2005)
[25] Vickers, A.: Whose data set is it anyway? Sharing raw data from randomized trials. Trials 7, 15 (2006)
[26] Hrynaszkiewicz, I., Altman, D.G.: Towards agreement on best practice for publishing raw clinical trial data. Trials 10, 17 (2009)
[27] Schaffer, A.: Your Medical Data Online: Google and Microsoft are offering rival programs that let people manage their own health information. Technology Review (July/August 2008)
[28] Singer, E.: Personal Medical Monitoring: Keeping tabs on your vitals with Microsoft HealthVault. Technology Review (April 24, 2009)
[29] Harris, L.: Google Health Heads to the Hospital: A new partnership at a Boston hospital could forecast future success. Technology Review (May 28, 2008)
[30] Weitzman, E.R., Kaci, L., Mandl, K.D.: Acceptability of a personally controlled health record in a community-based setting: implications for policy and design. J. Med. Internet. Res. 11, e14 (2009)
[31] Groves, T.: Managing UK research data for future use. BMJ 338 (2009)
[32] Halamka, J.: Blog Entry: A Privacy Framework for Personal Health Records, December 17. Blog (2008)
[33] Chhanabhai, P., Holt, A.: Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. Med. Gen. Med. 9, 8 (2007)
[34] Robinson, N., Graux, H., Botterman, M., Valeri, L.: Review of the European Data Protection Directive. TR7 10-ICO, Cambridge, UK, Rand Europe (2009)
[35] Halliday, D., Dizon, M., Kemmitt, H.: Baker & McKenzie's regular article tracking developments in EU law relating to IP, IT and telecommunications. Computer Law and Security Report 23, 227–232 (2007)
[36] Connecting For Health. Common Framework for Networked Personal Health Information. Connecting for Health Website (2009); The Markle Foundation, 7-6-0090