Public standards and patients' control: how to keep electronic medical records accessible but private

Kenneth D Mandl, Peter Szolovits, Isaac S Kohane

A patient's medical records are generally fragmented across multiple treatment sites, posing an obstacle to clinical care, research, and public health efforts.[1] Electronic medical records and the internet provide a technical infrastructure on which to build longitudinal medical records that can be integrated across sites of care. Choices about the structure and ownership of these records will have profound impact on the accessibility and privacy of patient information. Already, alarming trends are apparent as proprietary online medical record systems are developed and deployed. The technology promising to unify the currently disparate pieces of a patient's medical record may actually threaten the accessibility of the information and compromise patients' privacy.[2] In this article we propose two doctrines and six desirable characteristics to guide the development of online medical record systems. We describe how such systems could be developed and used clinically.

Summary points

- Electronic medical record systems should be designed so that they can exchange all their stored data according to public standards
- Giving patients control over permissions to view their record—as well as creation, collation, annotation, modification, dissemination, use, and deletion of the record—is key to ensuring patients' access to their own medical information while protecting their privacy
- Many existing electronic medical record systems fragment medical records by adopting incompatible means of acquiring, processing, storing, and communicating data
- Record systems should be able to accept data (historical, radiological, laboratory, etc) from multiple sources including physician's offices, hospital computer systems, laboratories, and patients' personal computers
- Consumers are managing bank accounts, investments, and purchases on line, and many turn to the web for gathering information about medical conditions; they will expect this level of control to be extended to online medical portfolios

Division of Emergency Medicine, Children's Hospital, 300 Longwood Avenue, Boston, MA 02115, USA

Kenneth D Mandl *director, clinical research*

Isaac S Kohane *director, informatics programme*

Laboratory for Computer Science, Medical Decision Group, Massachusetts Institute of Technology, Cambridge, MA, USA

Peter Szolovits *professor*

Correspondence to: K D Mandl Kenneth_Mandl@Harvard.edu

BMJ 2001;322:283–7

Medical information: access and privacy

No single institution can hope to encompass a patient's entire record. Ideally, it should be possible to create or assemble each patient's personal health record so that it is accessible at all points of care within the health service and contains data from all institutions involved in that patient's care. Two main impediments stand in the way of this ideal. Firstly, most healthcare institutions do not provide effective access for patients to their own data and, despite technical feasibility,[3] they show little willingness to share data with their competitors.[4] Secondly, patients are becoming increasingly anxious about the privacy of their medical records.[5] Such concerns seem justified when one considers that, under current laws and practices, identifiable medical data are routinely shared with insurance companies, government, researchers, employers, state bureaus of vital statistics, pharmacy benefit managers (companies that track doctors' drug prescriptions), local retail pharmacies, attorneys, and others.[6]

Doctrines for developing electronic medical records

We propose two doctrines to guide the development of electronic medical records: firstly, that record systems should be designed so that they can exchange all their stored data according to public standards and, secondly, that patients should have control over access and permissions. Building software compliant with public standards will enable connectivity and interoperability—even of diverse systems. Patients' control will allow protection of privacy according to individual preferences and help prevent some of the current misuses of personal medical information. The purpose behind these doctrines is to ensure long term access of patients and care providers to medical records for clinical use while minimising the risk to patients' privacy.

Public standards

Some of the stresses on the doctor-patient relationship could be eased by using computerised and internet based tools for decision support, communications,[7 8] and documentation.[1] As medical care increasingly depends on computerisation, software engineering and marketing practices become more relevant to issues of healthcare delivery and patients' rights. Unfortunately, many current systems fragment medical records by using incompatible means of acquiring, processing, storing, and communicating data. These incompatibilities may result from a failure to recognise the need for interoperability or they may be deliberate, with the aim of locking consumers into using a particular system. Either way, the practice precludes sharing of data across different applications and institutions.

The alternative to proprietary methods is the use of open standards. At minimum, open standards should be used in the exchange of information among different systems. For example, HL7 (Health Level Seven) is a voluntary consensus standard for electronic data

BMJ: first published as 10.1136/bmj.322.7281.283 on 3 February 2001. Downloaded from http://www.bmj.com/ on 20 April 2024 by guest. Protected by copyright.

exchange in healthcare environments.[9] It defines standard message formats for sending or receiving data on patient admissions, registration, discharge, or transfer; queries; orders; results; clinical observations; and billing. Using an open messaging standard such as HL7 allows different health applications, such as a laboratory system and a record system, to "talk" to each other.

Other standards have been adopted for various other data exchanges: DICOM defines messages for encoding and exchanging medical images, and X12 is a recent set of standards for exchanging authorisation, referral, and billing records. Standards such as CorbaMED try to define universal object models that can be widely used among different interoperating systems. Programs that exchange data according to open standards may nevertheless store and use those data internally in proprietary ways.

For different systems to share data effectively, they must all use at least a common set of communication protocols and message formats and allow the import and export of all their data. Common data structures and open source programming can foster the possibility of effective data exchange among systems.

Patient control

Substantial problems arise if patients cannot trust that their medical data will be used only in the ways they intend. If patients feel that they have no control over the fate of their medical information, they might fail to disclose important medical data or even avoid seeking medical care because of concern over denial of insurance, loss of employment or housing, or stigmatisation and embarrassment. Expectation of privacy allows trust and improves communications between doctors and patients.[10 11]

Patients are poised to take control of their personal medical information.[12] People are already managing bank accounts, investments, and purchases on line, and many use the web for gathering information about medical conditions.[13] Consumers will naturally expect to extend this control to online medical portfolios.

The fact that patients have trouble accessing their medical information while that very information is being used for unregulated secondary uses has exacerbated worries about the confidentiality and proper use of that record. A particular concern about online medical data is that companies providing the record software or maintaining the record systems want to own the patients' data. Giving patients control over permission to view their record—as well as over its creation, collation, annotation, modification, dissemination, use, and deletion—is key to ensuring patients' access to their own medical information while protecting their privacy.

Desirable characteristics of electronic medical records

In order to comply with the doctrines of public standards and patient control, designers of medical record systems should strive to imbue their products with the following characteristics.

Comprehensiveness

Because care is normally provided to a patient by different doctors, nurses, pharmacists, and ancillary providers, and, with the passage of time, by different institutions in different geographical areas, each provider must be able to know what others are currently doing and what has previously been done. Outpatient records should contain, at least, problem lists, procedures, allergies, medications, immunisations, history of visits, family medical history, test results, doctors' and nursing notes, referral and discharge summaries, patient-provider communications,[14] and patient directives. The records must also span a lifetime, so that a patient's medical and treatment history is available as a baseline and for retrospective analysis.

Accessibility

Medical records may be needed on a predictable basis (as at a scheduled doctor's visit) or on the spur of the moment (as in an emergency). They may be needed at a patient's usual place of care or far from home. They may be needed when the patient can consent to their use or when he or she is unconscious and only personal or societal policy can dictate use. Ideally, the records would be with the patient at all times, but alternatively they should be universally available, such as on the world wide web. In addition, with patients' permission, these records should be accessible to and usable by researchers and public health authorities.

Interoperability

Different computerised medical systems should be able to share records: they should be able to accept data (historical, radiological, laboratory, etc) from multiple sources, including doctors' offices, hospital computer systems, laboratories, and patients' personal computers. Without interoperability, even electronic medical records will remain fragmented.

Confidentiality

Patients should have the right to decide who can examine and alter what part of their medical records.[2 10] In principle a patient might choose to allow no access to such records, though at the risk of receiving uninformed and thus inferior care. At the other extreme some might have no hesitation in making their records completely public. For most patients, the appropriate degree of confidentiality will fall in between and will be a compromise between privacy and the desire to receive informed help from medical practitioners. Because an individual may have different preferences about different aspects of his or her medical history, access to various parts of the record should be authorised independently. For example, psychiatric notes may deserve closer protection than immunisation history. Further, patients should be able to grant different access rights to different providers, based either on their role or on the particular individual. Most patients will probably also choose to provide a confidentiality "override" policy that would allow an authenticated healthcare provider in an emergency to gain access to records that he or she would not normally be able to, though at the cost of triggering an automatic audit.

BMJ: first published as 10.1136/bmj.322.7281.283 on 3 February 2001. Downloaded from http://www.bmj.com/ on 20 April 2024 by guest. Protected by copyright.

Accountability

Any access to or modification of a patient's record should be recorded and visible to the patient. Thus, data and judgments entered into the record must be identifiable by their source. Patients should be able to annotate and challenge interpretations in their records, though we believe they should not be able to delete or alter information entered by others. Patients should also be able to see who has accessed any parts of their record, under what circumstances, and for what purpose. Reliable authentication is essential to make this feasible. Appropriate laws can reinforce accountability built into the records system.

Flexibility

We believe that most people want to make data about themselves available to those genuinely trying to improve medical knowledge, the practice of medicine, the cost effectiveness of care, and the education of the next generation of healthcare providers. This altruism has limits, however, when patients feel the threat of exploitation, the risk to privacy, or the annoyance of unsolicited follow up contacts. Patients should therefore be able to grant or deny study access to selected personal medical data. This can be based on personal policies or decisions about specific studies. An example policy might say that any study may use data if they will be stored only in aggregated, non-identifiable form.

Patients may also agree to more intrusive participation in specific studies. Whether patients are willing to be solicited on the basis of characteristics of their record should also be controllable. Patients could provide time limited keys to other parties to access a specified segment of their record. For example, they could permit hospitals to write to (but not read) the laboratory results section of their record. Or they could provide public health authorities with access to their immunisation history. All these patient functions should be accessible from any web browser in the world.

Challenges and limitations for electronic medical records

We are, with colleagues, implementing a patient controlled medical record system that follows our doctrines. Called PING (Personal Internetworked Notary and Guardian),[15 16] it was developed under the Federal Next Generation Internet Initiative.[17 18] We face important challenges in implementing personally controlled systems on a large scale. No matter how well these are integrated with institutional information systems, it is unlikely that patient controlled records would entirely replace provider or hospital based records. For important clinical, financial, and medicolegal reasons, providers need control over their own version of patients' medical histories. However, it is quite possible that, with appropriate consent and access privileges, portions of the personally controlled records would be downloaded into the institutional record to complement the existing data.

No matter how sophisticated security systems become, people will always manage to defeat them. If by no other means, they may be able to exploit human weakness to subvert someone with legitimate access to the data. Fortunately, technical advances in security systems for electronic records should continue to be driven forward by the commercial interests of companies doing business over the internet. In fact, we may need considerable further evolution of accepted policies and laws so that patients are not coerced into signing away their privacy rights to obtain care or reimbursement.

The widespread adoption of patient controlled health records that we propose will depend on solutions being found to several challenging technical and policy issues. No computer system has ever remained operational for the lifetime of a typical person; hence we will need procedures to migrate records to new computer systems and architectures. The contentious issue of how patients may be uniquely identified might entangle our design choices and desire for a distributed system of records. We will need to develop acceptable procedures for backing up data, anticipating recovery in case of disasters, agreeing on whether emergency overrides of patient's policies are ever acceptable, whether it is possible to retract access to data once it has been given, who is trusted to conduct audits and what rights they have to sanction violators of policy, and many other procedures.

Conclusions

Computerised medical information systems are at the start of what promises to be a rapid evolution.[19] We are still in a position to look ahead and consider the promise and pitfalls of such systems as we design and deploy them. We need not feel wedded to the structure and processes of current systems. In fact, it seems increasingly unlikely that an electronic longitudinal medical record will be produced as an outgrowth of the traditional institutional medical record.

In order for electronic medical records to eliminate the fragmentation of health information, be universally accessible, and guard patients' privacy, systems must be built according to public standards and controlled by patients.

Funding: This work was supported by the National Library of Medicine Next Generation Internet Initiative Contract N01-LM-9-3536 and by a grant from the National Library of Medicine, 1 R01 LM06587-01.

Competing interests: None declared.

1 Computer Science and Telecommunications Board, National Research Council. *Networking health: prescriptions for the internet.* (prepublication copy). Washington, DC: National Academy Press, 2000.
2 Hodge JG Jr, Gostin LO, Jacobson PD. Legal issues concerning electronic health information: privacy, quality, and liability. *JAMA* 1999;282:1466-71.
3 Van Wingerde FJ, Schindler J, Kilbridge P, Szolovits P, Safran C, Rind D, et al. Using HL7 and the world wide web for unifying patient data from remote databases. *Proc AMIA Annu Fall Symp* 1996:643-7.
4 Kohane IS, van Wingerde FJ, Fackler JC, Cimino C, Kilbridge P, Murphy S, et al. Sharing electronic medical records across multiple heterogeneous and competing institutions. *Proc AMIA Annu Fall Symp* 1996:608-12.
5 Harris-Equifax. *Consumer privacy survey, conducted for Equifax by Louis Harris and Associates in association with Dr Alan Westin of Columbia University*. Atlanta, GA: Equifax, 1996.
6 Computer Science and Telecommunications Board NRC. *For the record: protecting electronic health information.* Washington, DC: National Academy Press, 1997.
7 Mandl KD, Kohane IS, Brandt AM. Electronic patient-physician communication: problems and promise. *Ann Intern Med* 1998;129:495-500.
8 Ferguson T. Digital doctoring—opportunities and challenges in electronic patient-physician communication [editorial]. *JAMA* 1998;280:1361-2.
9 Health Level Seven (HL7). www.HL7.org (accessed April 2000).
10 Gostin L. Health care information and the protection of personal privacy: ethical and legal considerations. *Ann Intern Med* 1997;127:683-90.

BMJ: first published as 10.1136/bmj.322.7281.283 on 3 February 2001. Downloaded from http://www.bmj.com/ on 20 April 2024 by guest. Protected by copyright.

11 Institute for Health Care Research and Policy, Georgetown University. Health privacy project. 1999. www.healthprivacy.org/ (accessed 29 Nov 2000).
12 Ferguson T. Health online and the empowered medical consumer. *Jt Comm J Qual Improv* 1997;23:251-7.
13 Winker MA, Flanagin A, Chi-Lum B, White J, Andrews K, Kennett RL, et al. Guidelines for medical and health information sites on the internet: principles governing AMA web sites. American Medical Association. *JAMA* 2000;283:1600-6.
14 Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic-Patient Electronic Mail. *J Am Med Inform Assoc* 1998;5:104-11.
15 United States National Library of Medicine. Next generation internet phase II awards; 1999. www.nlm.nih.gov/research/ngisumphase2.html (updated 10 Dec 1999).
16 Riva A, Mandl KD, Oh DH, Szolovits P, Kohane IS. The personal internetworked notary and guardian. *Int J Med Inf* (in press).
17 Shortliffe EH. Health care and the next generation internet [editorial]. *Ann Intern Med* 1998;129:138-40.
18 Next Generation Internet Initiative. NGI Initiative home page. www.ngi.gov (accessed 29 Nov 2000).
19 Bates D. Commentary: quality, costs, privacy, and electronic medical data. *J Law Med Ethics* 1997;25:111-2.

(Accepted 3 October 2000)

Commentary: Open approaches to electronic patient records

David Markwell

Clinical Information Consultancy, Reading RG30 2SN
David Markwell
principal consultant
david@clinical-info.co.uk

Mandl and colleagues' vision of a longitudinal electronic health record providing individual patient information when and where needed is underpinned by two principles—the need for public standards and the need to respect patients' right to privacy. These issues are at the heart of any coherent approach to electronic patient records. The internet introduces a global dimension, limiting the longevity of isolated national initiatives. It is therefore timely that this US article raises key issues that should command general interest.

The authors refer to the efforts of HL7 to develop public standards for health communication. In Europe CEN TC251 (European Committee for Standardization, Technical Committee for Health Informatics) undertakes similar activities, and a four part, preliminary standard on communication of electronic healthcare records was adopted in June 1999.[1] This has been the basis for prototype messages in the NHS, including one for communication of records between general practice computer systems validated by clinicians and developers.[2]

Cooperation between European and US bodies on standards was formalised early this year by a memorandum of understanding signed by CEN TC251 and HL7. Convergence has been accelerated by the formation of HL7 affiliate organisations in many European countries, including Britain.[3] The main efforts in developing standards for medical records are now based on common methods and common technical solutions such as extensible markup language (XML). This follows global trends towards public, web based standards and is in full accord with the UK e-government interoperability framework.[4]

The foundations are in place for public standards on which to base communication of electronic records. However, views on the shape of standard records differ in emphasis: some anticipate records consisting of a collection of web documents, whereas others emphasise the importance of coded structured data that can be retrieved for aggregation, analysis, and decision support. The challenge is to build on the strengths of both approaches to develop record systems that are useful as well as user friendly. These systems must serve the wide range of purposes identified in the recent study of electronic patient records for primary care[5] and should have the attributes identified in the Institute of Medicine's 1991 report of computer based patient records.[6] Patient record systems must allow clinical statements to be faithfully recorded and retrieved, taking account of the interplay between record structure, terminology, and context.

Mandl and colleagues address the question of privacy by proposing a personal health record controlled by patients themselves. Data protection legislation in Europe[7] and the Caldicott report's guidelines for the NHS[8] differ from the rules applicable in the United States, but the need for a balance between privacy and legitimate demands for information is international. Patients' control of records solves some problems but may prevent professionals from accessing the information they need in order to fulfil, or show that they have fulfilled, their responsibilities.

The legitimate uses of patients' records are diverse, so it may be premature to adopt a single, all purpose electronic record for every patient. A single widely accessible, comprehensive patient record is not a substitute for appropriate communications, such as concise referral notes or discharge summaries. The immediate priority is to ensure that electronic records are fit for the purposes for which they are used. As the authors argue, common communication protocols and message formats based on publicly available standards are a prerequisite for any further progress in electronic patient records.

1 European Committee for Standardization, Technical Committee for Health Informatics. CEN/TC251. www.centc251.org (accessed 29 Nov 2000).
2 Markwell DC, Fogarty L, Hinchley A. Validation of a European message standard for electronic health records. In: Kokol P, Zupan B, Stare J, Premik M, Engelbrecht R, eds. *Medical informatics Europe '99*. Amsterdam: IOS Press, 1999:818-23.
3 HL7-UK (Health Level Seven UK). www.hl7.org.uk (accessed 29 Nov 2000).
4 Cabinet Office, Central IT Unit. e-Government interoperability framework. www.citu.gov.uk/egif.htm (updated Sep 2000).
5 NHS Executive. ScopeEPR—Royal College of General Practitioners Health Informatics Task Force electronic patient record study. www.schin.ncl.ac.uk/rcgp/scopeEPR/report/index22.htm (updated 13 Jul 2000).
6 Dick RS, Steen EB, eds. *The computer-based patient record: an essential technology for health care*. Washington, DC: National Academy Press, 1994:recommendation 1.
7 Council of Europe. *Convention for the protection of individuals with regard to the automatic processing of personal data (European treaty series No 108)*. Strasbourg: Council of Europe, 1981. (www.coe.fr/eng/legaltxt/108e.htm#debut)
8 Department of Health. *Report on the review of patient-identifiable information (Caldicott committee)*. London: DoH, 1997.

BMJ: first published as 10.1136/bmj.322.7281.283 on 3 February 2001. Downloaded from http://www.bmj.com/ on 20 April 2024 by guest. Protected by copyright.

Commentary: A patient's viewpoint

Rhona MacDonald

I still blush with embarrassment when I remember the horror of lying in a hospital bed and listening to my medical history being discussed by all and sundry. Doctors, nurses, medical students, pharmacists—everyone, it seemed to me—were poring over my open hospital notes with enthusiastic curiosity. I suppose even the cleaner could have had a look had she been so inclined. However, I also recall the frustration of being pointlessly reinvestigated because I had been referred to a different consultant who didn't have access to my old notes. This resulted in repeated invasive investigations, *x* rays, and scans and on one occasion being bled for 17 tubes of blood in the one sitting, a record even for me.

Here is my dilemma. I want my notes to be strictly confidential but readily accessible to those who need them. Electronic notes, while potentially solving my second problem, sets alarm bells ringing with regard to the first. I am not a technophobe, but I am wary of giving out personal financial information over the internet, and the thought of my entire medical history floating somewhere in cyberspace doesn't fill me with confidence. Perhaps I have seen too many films about ingenious hackers.

Even if I can get over my suspicion of electronic notes, new dilemmas arise. According to Mandl and colleagues, I will be able to choose who I want to look at my notes, what bits I want them to look at, and, finally, whether I want to provide an "override" policy that would allow a healthcare worker to confound my carefully thought out plan in an emergency and gain access to records that he or she would not normally be authorised to see. Call me suspicious, but what is to stop those who want access to my notes against my wishes declaring an emergency and pressing that button whenever they feel like it? To be fair, the authors do say that I will be able to see who has accessed my record and under what circumstances, but by that stage it might be a bit late.

The best bit is that I will be able to annotate and disagree with interpretations in my records, although I will not be able to alter or delete them. Wow! I bet this will have doctors in Britain reeling in horror. Not only will I be able to read my own notes but I can disagree with what is written about me and discuss it with my doctor. I think that, in Britain at least, the doctor-patient relationship will have to come a long way before doctors are willing to give patients this amount of autonomy. I would be delighted, however, if this ever became a reality.

In conclusion, I don't want much—just for my medical records to be seen only by those whom I authorise, and for the records to be readily accessible to them wherever they are. My medical history may not mean much to others, but it is an important part of my life and I would like others to treat it with the respect it deserves. Also, thanks to this article putting the notion in my head, I would like a bigger say in what goes into my notes, and if I don't like something I would like it taken out. Somehow I think I will have to wait a long time for that to happen. Maybe electronic notes like those described are the way forward, but at the moment I view them with optimistic scepticism.

BMJ
Rhona MacDonald
editorial registrar

rmacDonald@bmj.com

A sense of déjà vu

The room was homely, nestled in the basement, and traversed by pipes encased in silver foil. With a sense of the inevitable I settled down. The clerks, now ignoring me, continued their cheery boasts of difficult finds and commiserations on last minute telephone requests. Record systems are not difficult to master—colour codes, consecutive numbers, paired or in reverse, always some quirk—but the real problem is those booked out eons ago which force a trail round distant departments. At least this time mine were waiting and marked for my attention. I was interested to see what I could glean about a recent waiting list initiative for suspected colorectal cancer, but I wondered, dispiritedly, why the mechanics of audit remained the same despite all the investment and talk.

Out of clinical practice for several years, however, I was soon fascinated by an array of tummy troubles, and developing again that sense of competence in retrieving deeply buried histology results and GP referral letters. But the records now seemed swollen. Care plans, charts, protocols, explanations, detailed summaries, forms relinquishing hospital responsibility, all stuffed into those never-to-be-filed pockets of history.

However, as my archaeology continued, these gave way to the slimmer volumes of older patients rarely in hospital. Letters of only three sentences described the positive features of diagnosis and management. What a joy to audit these. Their tissue-thin slips and uneven typewritten ink conjuring up an old NHS of no-nonsense doctors and grateful patients.

And then in 1957 I found it—from a senior registrar to a young woman previously attending the gynaecology clinic:

"Dear Mrs X,

I find that your name is still on the waiting list and that you have not yet been admitted to hospital for your operation. Would you please indicate on the attached form whether (a) you still have the same trouble, (b) still wish to be admitted to hospital, or (c) have received treatment elsewhere, by striking out the words which do not apply in your case.

1 My symptoms continue/have disappeared.
2 I still wish/do not wish to be admitted to hospital.
3 I have/have not received treatment elsewhere.

Please return the stamped addressed envelope provided."

Mrs X had replied in a small, careful hand that she was well and did not need an operation, thank you.

An early example of patient-centred decision making or the discovery of a 40-year cycle in waiting list initiatives?

Elizabeth Davies *specialist registrar in public health, East Surrey Health Authority*

We welcome articles of up to 600 words on topics such as *A memorable patient, A paper that changed my practice, My most unfortunate mistake*, or any other piece conveying instruction, pathos, or humour. If possible the article should be supplied on a disk. Permission is needed from the patient or a relative if an identifiable patient is referred to. We also welcome contributions for "Endpieces," consisting of quotations of up to 80 words (but most are considerably shorter) from any source, ancient or modern, which have appealed to the reader.

BMJ: first published as 10.1136/bmj.322.7281.283 on 3 February 2001. Downloaded from http://www.bmj.com/ on 20 April 2024 by guest. Protected by copyright.