Security requirements for a lifelong electronic health record system based on non-standard ethical principles

Jacques Wainer Carlos José Reis de Campos
Daniel Sigulem

Department of Health Informatics, UNIFESP, Brazil

version of Aug 2006

Abstract

This paper discusses the security requirements of a centralized, unique electronic health record. The requirements are based on the well known principles of confidentiality and integrity, and the less discussed principles of control and legal value. Among the non-standard ethical principles, we argue that patients should not have the right to change or read their health records, against, for example, the IMIA code of ethics. The paper does not discuss any technical or legal solutions to the priciples proposed herein.

1 Introduction

There is a large body of literature regarding the security concerns of electronic patient medical records. These papers range from theoretical models for cryptographic or access control mechanisms (for example [1, 2]), description of different implemented systems (for example [3]), description of different national experiences (for example [4, 5, 6]), to practical comparisons between different standards, to guidelines to implement a particular security standard (for example [7, 8]). But most of these papers are mainly concerned with the confidentiality aspect of the records - that no unauthorized party should have read access to it. We discuss in this paper that there is a more complex set of requirements regarding integrity, control, legal aspects, and other aspects of an integrated health record system. Furthermore, in this paper we challenge some of the ethical principles that justify some of the security requirements that have been proposed to electronic patient records, specially the principle that the patient should have the right to access and change his own medical records (as proposed by the IMIA ethics code [9]).

In this paper we assume a single computer accessible record of **all** of a person's health events. We use the term **electronic health record** or **EHR** for such a system. The EHR should be contrasted with a computer record of the patient's health events which is kept/controlled/mantained by a single health organization. We call this second form the **electronic patient record** or **EPR**. EPR are maintained by a particular health organization and contain the patient health data while in the care of that organization - thus there will be different EPR for a particular patient at a local hospital, where he performed a minor surgery, at a distant hospital where he was treated for a car accident, at his current and past family physicians, at his current and past dentists, at his analyst, and so on, which reflects the current situations in most part of the world.

The idea of a single, unique, Internet accessible (with severe restrictions – see below) electronic health record has been mentioned many times in the literature [10, 6, 4, 11, 12, 13, 14]. In this paper we will discuss the requirements of such EHR system on a conceptual level, with no regard if there are technologies or policies or laws that are able to implement these requirements.

In this paper, besides EHR and EPR we will use the abbreviation **HP** for **health professional**, which includes all sorts of professionals that can have access to the patient's EHR including physicians, nurses, dentists, psychologists, alternative medicine practitioners, and so on (please see multiple entry principle below). We will also use the abbreviation **HO** for **health organization**, which includes organizations ranging from a single professional clinic to hospitals.

We believe that the central point of an EHR is to gain quality and efficiency in caring for the patient. The patient's health conditions and his whole health history is available to the health professional to aid in diagnostic, therapy planning, and care of the patient. This aid can be of three main forms: provision of essential patient health information, efficiency by reusing of previous laboratory exams, and opportunistic increases in quality. We will discuss these three forms of aid shortly.

Furthermore, the EHR serves as the record of a health professional's actions on behalf of that patient and should be the unique and definite source of information regarding those actions, for legal and professional purposes. Thus, if some professional or legal body is evaluating the HP's competence, the actions and notes the HP recorded in the EHR of his patients should be the definite source of information.

The paper is organized as follows: section 2 discusses the general principles of confidentiality, control, integrity and legal value, and the goals of a EHR. It is important to point out that the general principles of confidentiality and integrity are well known and well discussed in the literature (see section 7), but we feel it is important to list them with other less well known and less discussed principles for the sake of completeness. Section 3 discusses the subprinciples related to integrity. Section 4 discusses the subprinciples related to confidentiality and control and section 5, the subprinciples related to the legal value of the EHR. Section 6 discusses other principles of a more practical nature, which we feel are also very important. Section 7 discusses some of the literature on these

issues and finally section 8 discusses some open issues. This paper does not propose any technical, or legal solutions to the principles proposed. If these principles are accepted, that will be the result of the efforts of many researchers and research programs.

2 Generic Principles

We assume the following generic principles for the EHR:

- **confidentiality**: the patient's records are private and confidential; no unauthorized person may inspect the contents of the patient's records.
- **control**: the patient controls the access to his records. A patient may grant access to a health professional and revoke such access rights when the treatment is over.
- **integrity**: the patients life may depend on the data contained in the records, and thus only authorized people can enter or change the data.
- **legal value**: the patient's records are the unadulterated, complete record of all actions taken by the health professionals on behalf of that patient, and should be the definite source of information regarding said actions.

These general principles of confidentiality, control, integrity, and legal value will be further elaborated and discussed below. The certainties expressed above will be relativized as we further elaborate the ethical and practical principles.

In general terms, confidentiality and control are patient-related principles. Since health information can be used to cause losses to a patient, it is the patient's needs that are served by confidentiality and control. Confidentiality allows the patient to be sure that no one but authorized people can **read** his records, and control allows the patient to **grant** to an HP read and write access to his medical reconds, and then **revoke** the access when he feels the HP should have no longer access to it.

Integrity is a health professional related property, and thus, we believe, it is very relevant for the appropriate use of the EHR. The whole point of a EHR is to improve the quality and efficiency of the professional's work, and for that integrity is absolutely necessary.

Finally, legal value is a very important aspect of the EHR, and not a secondary aspect as it is sometimes assumed. The EHR should be the definite source of information regarding the health professionals's actions on behalf of the patient.

2.1 Uses of the EHR

Medical records, specially paper based records, have a double use: they serve as a legal document that records the HP and the HO's actions, and as a written collaboration medium among HPs (in case the patient is being treated by multiple HPs), or as a reminder tool for single HP across time.

A centralized, lifelong EHR has another use - to improve the quality of the HP's actions and decisions by providing relevant patient health data, and by potentially providing economy for the patient treatment through the reuse of exam's results.

The most important aspect of the EHR is that it should record the **current, relevant aspects of the patient health**, including:

- current diseases
- current complaints
- allergies and other health conditions
- medications being taken

and so on. The current health aspects of the EHR improves the quality of the patient care by helping the HP to avoid drug interaction problems, recognize iatrogenic symptoms, avoid allergic reactions to drugs, interpret exams results, and so on.

Furthermore, the EHR contains all **recent laboratory exams** of the patient. If the patient had a recent blood sugar test which shows normal sugar levels, if those results are recent enough that they are still valid, and if doctor *trusts* the laboratory which performed the exam and trusts the record, then there is no need to ask for a new exam.

Finally the EHR should contain the **long term patient medical history**. For example, by having all blood sugar measures of the patient in a single place, an HP may opportunistically realize that the patient has some sort of blood sugar pattern that may indicate a potential problem. Or that a current complaint can be attributed to the long term consequences of a disease the patient believe was cured long time ago. Thus, there may be an improvement of quality on the HP decision based on the opportunistic use of information stored in the medical history of patient.

2.2 Comparing with electronic patient records

Electronic patient record (EPR) is a more localized medical record, kept in electronic form. It is usually controlled, or owned by a health care organization and its purpose is similar to the paper based medical record - a legal document and a collaboration/remind tool.

The literature on EPR focus mainly on the confidentiality issue. A search on August 2006 on PUBMED for the keyword "Medical Records Systems, Computerized"[MAJR] and some other keywords such as "privacy", "confidentiality", "integrity" and so on, resulted in the number of articles listed in table 1.

Integrity is assumed to be a responsibility of the owner of the records, and thus a somewhat "obvious" requirement. Confidentiality, as we discussed above, is a requirement that serves the patient, and not the health organization, and thus a requirement that must be imposed by legislation or by some other external constraints.

keyword	number of articles
none	7591
confidentiality	1027
privacy	539
availability	119
integrity	83

Table 1: Result of queries in PUBMED regarding EPR

Control is an irrelevant issue in EPR - if the patient chooses a particular HO he is implicitly giving this HO the right to create and manage his EPR. But usually, the patient does not have the right to control who within the HO should have which access to his records - again by choosing an HO, he is implicitly accepting whatever delegation of access control the HO has in place.

We are not aware of much discussion regarding the legal value of the EPR. Clearly all HO are aware of the legal aspects of the records, specially requirements such as compliance with national regulations regarding the storage of records, and so on. But, in this paper, legal value is the aspect of the records that defines it as the only source of information regarding the HP actions.

3 Integrity issues

As we mentioned before, we believe that the integrity aspects of the EHR are the most important ones for its purpose, which is to provide the information to improve care quality, the possibility of economy, and the possibility of an opportunistic gain in quality. But in order to use the information, the HP must trust that the information is correct, and up-to-date.

The general principle of integrity is that no unauthorized person and no unintentional error should be able to add, remove, or change any data in the EHR. Besides integrity, the following principles are closely related:

Principle 1 ***Availability:*** *the EHR must be available when the HP needs it. Thus all care in making the system robust and redundant is necessary.*

Principle 2 ***Up-to-dateness:*** *The EHR must contain all of the latest relevant information regarding the patient's health; so there should be no significant delay from when data is entered into the record and when it becomes available to a different HP. If an HP prescribes some medication to the patient, that information must be included in the EHR as soon as possible, so if the patient consults another HP, for some other reason (see multiple entry points below), that information must be available.*

Furthermore, if the EHR is not current, the HP must know about it, so he can ask the patient about the missing information. For example, a properly authorized HP gained access to the patient's EHR but did not add any information to

it, which seems to indicate that the HP has not yet uploaded the records of the consultation to the EHR. The system should then inform the next HP that the patient's record is probably not current, so the HP can ask the patient about new drugs, diagnostics and so on that may have happened in the unrecorded consultation. Of course, the second HP cannot enter such data as the missing consultation, which is the responsibility of the first HP, but can take that information, as provided by the patient, into consideration.

Principle 3 ***Usability*** *Although usability is not a integrity issue, it is also central to the correct use of the EHR - an HP should not need to read through all of the patient's records to figure out that she has a drug allergy to Novocain which was diagnosticated 15 years ago during a dentist appointment. All relevant, current health conditions, including allergies, must be easily accessible, and presented in a clear way to the HP. Search facilities must also be provided in order to look for specific data in the patient's record.*

4 Confidentiality and Control issues

Confidentiality states that the patient may have expectations that no unauthorized party will be able to **read** his medical records. Thus, the storage and transmission of the EHR should be guarded by security measures that would prevent eavesdropping.

Control state that the patient can decide how should have access to his records and when this access is revoked. The patient grants access to his EHR to a health professional for a limited, but not predefined, duration. While that health professional is treating the patient he has access the EHR but as soon as the treatment is over, the HP's access to the records is closed.

This places the interesting question of when is a treatment over. In case of hospitalizations, there are activities that mark the end of the treatment, but in other cases, that is not so clear. Of course the patient may decide that the treatment is over because he no longer plans to visit the HP. In this case, there should be a way for the patient to revoke the HP's access to his EHR without attending the HP's office.

Another partial alternative is to grant access only during a consultation. That would preclude the HP accessing exams results which may have been entered into the EHR by a laboratory as soon as they are available, which could be very important in some cases. It would also preclude the HP from thinking about the patient's data outside the consultation, from discussing the case with a colleague and so on.

Principle 4 ***No access rights to the patient.*** *The patient has no right to read or change the EHR; the patient can only delegate access rights to his own records to health professionals. This is a controversial principle. We claim that EHR is a communication medium between health professionals; it is their ethical responsibility to mediate the access of the patient to the information contained there.*

This is, of course, a very polemic principle, that goes against the usually accepted requirements of electronic medical records. For example, this principle violates, for example, IMIA Code of Ethics for Health Information Professionals [9] the Principle of Access:

> The subject of an electronic record has the right of access to that record and the right to correct the record with respect to its accurateness, completeness and relevance.

We feel that the right to correct the records, as stated in the IMIA's Principle of Access, is profoundly misguided, and violates both the legal value and specially the integrity requirements of the record. For example, can a patient with Munchausen syndrome[1] be trusted to correct his own records for completeness and relevance?

Granting the patient only the right to read his own records also may pose some problems. Should a patient with fragile physique be able to read that his doctor is considering as a diagnostic hypothesis a serious, degenerative disease? Should the patient read in his records that he is taking a placebo medicine for his psychosomatic complaints? We feel that it is the health professional's ethical and professional responsibility to choose what and how to inform his patients. Some professional may choose to disclose all, some may not, but it is the HP's professional responsibility to make that choice.

We do not dispute that in most cases it is probably beneficial to the patient to have read access to his own records, but we believe that this should **not** be a system requirement.

Principle 5 ***Emergency access*** *There are reasonable situations in which a HP may access a patient's record without his previous authorization. This is particularly clear in emergency situations - if the patient comes to an emergency clinic unconscious or otherwise unable to grant access to his record, the responsible HP must be able to gain access to the records.*

Principle 6 ***Implicit acceptance of health organization structure.*** *By granting access to his EHR to an HO or to an HP, the patient implicitly accepts whatever delegation are in place in the HO or whatever delegations the HP defined. The HO and the HP may* after the fact *be criticized, or punished by these delegations, but the patient cannot control who will or will not within the HO, have access or what kind of access, to his EHR.*

In implicit acceptance of the HO's structure states that the patient will not grant the right to access his EHR to each member of the HO and will not be able to control who has what kind of rights to his EHR. If the patient grants the HO access to his EHR, he implicitly accepts whatever delegation structure is in place in the HO. This, of course, does not free the HO from adopting good security practices such as limiting the rights of HPs based on roles, attribution of rights based on the principle of least rights, and so on.

[1] Repeated fabrication of physical illness–usually acute, dramatic, and convincing–by a person who wanders from hospital to hospital for treatment [15].

Principle 7 ***Limited read access for public health, legal and professional entities*** *Some legal, public health, or professional bodies may have a limited and anonymized read access to the EHR* ***independent*** *the patient's approval.*

If an HP or an HO is being legally investigated or being reviewed by a professional body, these bodies may have read access to anonymized segments of the HP's patients records which refer to the HP's (or HO's) decisions and actions.

5 Legal value

As we discussed above, any medical record has a double goal - as the recoding of the patient's data and the recording of the doctor's medical actions. The legal value of the EHR concerns this second aspect - when challenged in the proper legal context, the doctor must be able to use parts of the EHR to justify his own decisions and actions. Thus, in the proper legal context, it should be possible to access a particular doctors medical actions as recorded in the EHR of a patient, independent of the patient's will on the subject.

Principle 8 ***Incrementability*** *The EHR should be incremental, that is, information can never be removed or altered from the record, only added. Of course, there are information that is wrongly entered, and thus there should be a mechanism to* add *a correction to the information already present. The record when presented to an HP will only show the corrected versions of the data, but as we will discuss later, the uncorrected version must be kept, as well as the correction, who made it, and when.*

Principle 9 ***Non repudiability*** *One cannot deny making an entry into a patient's EHR. This is an important requirement regarding the legal value of a record - if the record state that an HP decided on a particular therapy, or made a particular diagnostic, that record cannot be denied by the HP.*

Principle 10 ***Explicit delegations*** *In an HO, different professionals will enter different data to the patient's EHR. It should be clear in the record the identity of the person who entered the data, who delegated that right to the person, and so on.*

Principle 11 ***Recoverability of specific moments****. In order to verify the quality of an HP decisions and actions it is necessary to restore the EHR to the particular moment in time when the HP was performing the decisions and actions being reviewed. Thus the system must be able to show a snapshot of the EHR at that time; corrections and data entered after that moment must not be shown.*

6 Other practical considerations

Principle 12 ***Uniqueness of the EHR****. The only place in which the HP should have to enter data, decisions, and actions regarding the patient is the EHR. There should not be a second, local record, on which the HP add some sort of information regarding the patient.*

If the HP needs to write down some information regarding his medical actions on some other record, even if this record is confidential enough so that by itself it will not divulge the patient private information, there is the real risk that because of the double work, either the EHR or this second record will be incomplete. For example, if an hospital pharmacy is not linked to the EHR system, the HP will have to enter drug prescriptions twice, in the EHR and in the hospital pharmacy system. Such double record will likely result in the incompleteness of the EHR - there will be cases in which the HP will enter a drug prescription in the hospital system but not in the EHR.

Principle 13 ***Right of a record of one's own work.*** *The HP and the HO may have read access to an anonymized copy of the segment of the EHR which reflects their actions even if she has no longer access right to the record.*

This principle follows form the uniqueness principle above. HP and HO have legitimate use for information regarding the medical actions they undertook on behalf of the patient, including:

- billing
- research
- quality control

Thus, the HP and HP should be able to extract the appropriate segments that reflect their actions from the patient's EHR, instead of requiring HO to keep a second or third record for these purposes.

This is also a controversial right - the standard understanding is that the medical record is own by the patient, although the health organization or professionals may have the guard of it. But if the patient requests his records, the HP or HO may be left with no written record of their own work, which we feel is unfair to them.

Unfortunately, the three legitimate uses of patient information above have different requirement regarding the copy of the EHR. The research and quality control copies should be anonymized, but should contain enough previous information about the patient to be able to judge the quality of the actions performed, or at least to be able to place those actions in different contexts. Billing, on the other hand, needs identification but no previous information about the patient. Thus, care must be taken to avoid linking both copies, since that would disclose too much information about the patient.

We feel that in this case, the HP and HO should have a **copy** of the appropriate segments of the patient's EHR, instead of a limited read access to the record. The copy should be authenticated by the system, but is a copy because there is no reasons for the HP and HO to retain any access rights to the EHR.

Principle 14 ***Very long storage times*** *The EHR must last at least as long as the patient lives and probably longer, if there are controversies regarding the patient's death or last years. This places important constraints regarding storage of the data - the data must be readable even after decades of storage. But more relevant to this paper, the digital signatures must also remain valid for the corresponding period - so that data entered and digitally signed, must be able to be verified decades afterwards.*

Principle 15 ***Multiple entry points*** *On should not assume that the patient will have a single HP, or a single entry point to the health system, so that this entry point have some overall view of the patient. The patient may be consulting with different HPs in parallel.*

For example, the patient may see a gynecologist specialist on a yearly basis, may sporadically consult with a sports specialist who prescribes food supplements and a particular diet to achieve the patient's sport goals. The patient may also be seeing a orthopedic specialist for a back pain, and regularly consults a general practitioner regarding the control of her diabetes. Finally the patient also consults a fitotherapist how prescribes a set of herbal supplements for the patient's stress management.

The consequence of the multiple entry points principle is that the EHR cannot be held under the custody of a single HO for long. Even if the patient is admitted to an hospital, it is possible that he may grant read access to (one of) his private HP during his stay.

Principle 16 ***Substitutability of passwords and keys*** *It is unreasonable to think that a patient will remember his EHR password, or keep a smart card, for all his life. So there must be mechanism to generate a new password or keys for a patient (provided his identity has been established with the appropriate certainty). Even if the identification mechanism is based on biometric data, it is uncertain that some biometric data does not change with time.*

Principle 17 ***Technological diversity*** *One cannot expect that all HO have the same level of technology. For example, it may be unreasonable that all HO are always connected to the EHR servers - and thus may receive a message from the servers regarding changes in a particular patient record. A HO may only have a phone line through with it connects to the EHR servers,* when the HO needs. *Similarly, even if there is a biometric data which has been proven to not change along the lifespan of a person (regardless of health condition), it would be unreasonable to demand all HO to have the appropriate biometric reader.*

Principle 18 ***Different access patterns and need regarding the records.*** *Different health organizations will have different access needs regarding the EHR*

- if the patient is hospitalized, the access to his records are usually in parallel (different people entering and reading the data), in high volume (imaging and signal exams) and in high frequency. A clinic would require a very different pattern of access to the EHR.

This principle opens up the possibility of different optimizations techniques for different HO. For example, an hospital may lock the centralized EHR and maintain a local version of the records, and only upload it to the central when the patient is released.

7 Related research

A paper with similar concerns as this one is [16], which lists 28 principles regarding electronic medical records, compiled from ten policy documents and from US organizations (such as the National Research Council), and makes a comparative review among the different sets of principles. Principle 12 in [16], which states:

> Health care providers have the right to maintain private recordings of observations, opinions, and impressions whose release they consider could be potentially harmful to the well-being of the patient. They shall not disclose this information without due reflection on the impact of such release.

is particularly relevant to this paper, since is part of our justification for the no access rights to patients, which in turn contradicts principles 2, 3, and 4 (right to access, right to a copy and right to correct/amend one own record) of [16]. Principle 12 is also our justification regarding the health organizations right to a copy of the record of their own work.

[17] reviews the literature on the issue of benefits of the patient (read) access to his own record and concludes that although the studies were of limited quality, they show " modest improvements in doctor-patient communication, adherence, patient empowerment, and patient education". The study also points out problems of increase anxiety in making psychiatric records available to the patients. [18] reports on the benefits of providing read and a limited write access to the patient's EHR in terms of accuracy of the data and compliency with treatments.

[19] presents the tension between confidentiality of the EPR and the interest of public health surveillance, and discusses that anonymisation by itself in the situation in which there are multiple EPR for each patient would be a problem because of the duplicity of the data. In our proposal of a single EHR, those concerns would be less of a problem.

The major part of the literature regarding security requirements of EPR deal mainly with the confidentiality issues, with a minor part regarding integrity issues. [20] is an example of such confidentiality centered paper.

Our definition of EHR as a single, centralized life-long health record, is called Lifetime Health Record in [6], which describes the Malaysian plan for a

simplified EHR. The Malaysian LHR contains a summary of local EPR, and also provide anonymized information to public health bodies.

There is a large literature of EHR under the name of Personal Health Record [11, 12, 13, 14].

A different approach to our single, centralized EHR is to have local EPR that allow for some degree of interchangeability. A series of papers discuss the need for standards for interchanging and sharing EPR across different organizations, or countries (for example [21, 22, 23]).

Other research papers discuss different technical aspects relevant to the issues in this paper. [24] discusses the issue of the long period storage and its impact on the digital signatures in the EHR. In particular the paper proposes a re-signing mechanism that would replace "outdated" digital signatures by fresh ones. [25, 26] discuss issues and techniques for the anonymization of medical records.

Finally, to our knowledge [27] was the first paper to point out the requirement of recoverability of specific moments, but the paper discusses the difficulty in implementing this requirement when the EHR is just a set of pointers (or links) to health organization's specific data and processes.

8 Open issues

There are a large set of issues that are not discussed in this paper. First, we do not propose any implementation or technical solution to the security requirements herein. Solution to these requirements will certainly involve from complex cryptographic techniques, to trusted centralized servers, to operational procedures in HO, to national level legislation. We also do not discuss anything about the content of the EHR.

Another issue we did not address is the for how long the data should remain available in the EHR. The records of an ICU patient will contain a large amount of data regarding the patient's vital signs, that is very relevant while the patient is in care, and possible even after he has been released from the hospital care. But it is likely that such data is irrelevant 20 years from the fact, and should not be stored in the centralized EHR.

But more to the point of the ethical principles discussed, we feel that some issues require further discussion. One of them is whether the patient can ask for certain information to be private and not made available to other HP. The patient may tell a particular HP some information because he trusts the HP, and believe that the HP can make the appropriate use of that information on behalf of the patient. But the patient may not trust the entire health system, and thus may want that information not to be available to the other authorized HP.

Another complex ethical issue, for which we have no solution, is the linking of different patients records. Clearly, there are a large set of situations in which knowing the health conditions of the patient's parents will benefit the patient's care, and in a few other situations, knowing the spouse's health condition will

also help the patient's care. On the other hand, the parents or the spouse did not delegate to these HP the right to access their records.

References

[1] Marc Wilikens, Simone Feriti, Alberto Sanna, and Marcelo Masera. A context-related authorization and access control method based on RBAC. In *SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*, pages 117–124, New York, NY, USA, 2002. ACM Press.

[2] R. Chandramouli. A framework for multiple authorization types in a healthcare application system. In *17th Annual Computer Security Applications Conference (ACSAC'01)*, page 137. IEEE Computer Society, 2001.

[3] Bernd Blobel, Peter Pharow, Volker Spiegel, Kjeld Engel, and Rolf Engelbrecht. Securing interoperability between chip card based medical information systems and health networks. *International Journal of Medical Informatics*, 64:401–415, 2001.

[4] Knut Bernstein, Morten Bruun-Rasmussen, Sren Vingtoft, Stig Kjr Andersen, and Christian Nhr. Modelling and implementing electronic health records in denmark. *International Journal of Medical Informatics*, 74:213–220, 2005.

[5] Christian Nhr, Stig Kjr Andersen, Sren Vingtoft, Knut Bernstein, and Morten Bruun-Rasmussen. Development, implementation and diffusion of ehr systems in denmark. *International Journal of Medical Informatics*, 74:229–234, 2005.

[6] Jai Mohan and Raja Razali Raja Yaacob. The malaysian telehealth flagship application: a national approach to health data protection and utilisation and consumer rights. *International Journal of Medical Informatics*, 73(3):217–227, 2004.

[7] Bernd Blobel. Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics*, 73:251–257, 2004.

[8] Ross Anderson. Clinical system security: interim guidelines. *British Medical Journal*, 312(7023):109–111, 1996.

[9] IMIA. International Medical Informatics Association Code of Ethics for Health Information Professionals. http://www.imia.org/English_code_of_ethics.html. Accessed July 2005.

[10] Johan G. Beun. Electronic healthcare record; a way to empower the patient. *International Journal of Medical Informatics*, 69(2-3):191–196, 2003.

[11] Matthew I. Kim and Kevin B. Johnson. Personal health records. *Journal of the American Medical Informatics Association*, 9:171–180, 2002.

[12] Dean F. Sittig. Personal health records on the internet: a snapshot of the pioneers at the end of the 20th century. *International Journal of Medical Informatics*, 65(1):1–6, 2002.

[13] I. Iakovidis. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in europe. *International Journal of Medical Informatics*, 52:105–115, 1998.

[14] Ira C. Denton. Will patients use electronic personal health records? responses from a real-life experience. *Journal of Healthcare Information Management*, 15:251–259, 2001.

[15] Mark H. Beers and Robert Berkow, editors. *The Merck Manual of Diagnosis and Therapy*, chapter Chapter 185 - Psychiatry In Medicine. Merk and Co, Inc., 17th edition, 2005.

[16] Suzy A. Buckovich, Helga E. Rippen, and Michael J. Rozen. Driving toward guiding principles: A goal for privacy, confidentiality, and security of health information. *Journal of the American Medical Informatics Association*, 6(2):122–133, 1999.

[17] Stephen E. Ross and Chen-Tan Lin. The effects of promoting patient access to medical records: A review. *Journal of the American Medical Informatics Association*, 10:129–138, 2003.

[18] Maria Staroselsky, Lynn A. Volk, Ruslana Tsurikova, Lisa Pizziferri, Margaret Lippincott, Jonathan Wald, and David W. Bates. Improving electronic health record (ehr) accuracy and increasing compliance with health maintenance clinical guidelines through patient access and input. *International Journal of Medical Informatics*, 2005.

[19] Chris Verity and Angus Nicoll. Consent, confidentiality, and the threat to public health surveillance. *BMJ*, 324:1210–1213, 2002.

[20] Randolph C. Barrows and Paul D. Clayton. Privacy, confidentiality and electronic medical records. *Journal of the American Medical Informatics Association*, 3(2):139–148, 1996.

[21] Knut Bernstein, Morten Bruun-Rasmussen, Sren Vingtoft, Stig Kjr Andersen, and Christian Nhr. Modelling and implementing electronic health records in denmark. *International Journal of Medical Informatics*, 74(2-4):213–220, 2005.

[22] Amado L. Espinosa. Availability of health data: requirements and solutions. *International Journal of Medical Informatics*, 49:97–104, 1998.

[23] Marcel Lucas Muller, Frank Uckert, Thomas Burkle, and Hans-Ulrich Prokosch. Cross-institutional data exchange using the clinical document architecture (cda). *International Journal of Medical Informatics*, 74:245–256, 2005.

[24] Peter Pharow and Bernd Blobel. Electronic signatures for long-lasting storage purposes in electronic archives. *International Journal of Medical Informatics*, 74:279–287, 2005.

[25] Fred M. Behlen and Stephen B. Johnson. Multicenter patient records research: Security policies and tools. *Journal of the American Medical Informatics Association*, 6(6):435–443, 1999.

[26] Catherine Quantin, Francois-Andre Allaert, and Liliane Dusserre. Anonymous statistical methods versus cryptographic methods in epidemiology. *International Journal of Medical Informatics*, 60:177–183, 2000.

[27] Ab Bakker. Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. *International Journal of Medical Informatics*, 73(3):267–270, 2004.