Security Requirements for a Lifelong Electronic Health Record System: An Opinion

J. Wainer[*,1,2], C.J.R. Campos[2]. M.D.U. Salinas[2] and D. Sigulem[2]

[1]*Computing Institute, University of Campinas, Brazil*

[2]*Department of Heath Informatics, Federal University of Sao Paulo, Brazil*

Abstract: This article discusses the authors' views on the security requirements of a central, 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. The article does not discuss any technical or legal solutions to the requirements proposed herein.

Keywords: Security, electronic health record, health record, ethics.

INTRODUCTION

There is a large body of literature on the security concerns of electronic health record (EHR) systems. These articles range from theoretical models for cryptographic or access control mechanisms [1] to descriptions of different implemented systems [2], descriptions of different national experiences [3,4], practical comparisons between different standards, and guidelines for implementing a particular security standard [5]. But most of these articles are concerned mainly with the confidentiality aspect of the records: that no unauthorized party should have read access to them. As we discuss in this article, there is a more complex set of requirements regarding integrity, control, legal aspects, and other aspects of an integrated health record system.

In this article we assume a single computer-accessible record of all a person's health events. We use the term *electronic health record* (EHR) for such a system. The EHR should be contrasted with a computer record of the patient's health events that is kept, controlled, and maintained by a single health organization (HO). We call this second form the electronic patient record (EPR). EPRs are maintained by a particular HO and contain the patient health data while in the care of that organization; therefore, there will be different EPRs for a particular patient at a local hospital where he or she underwent minor surgery, at a distant hospital where he or she was treated for injuries sustained in a car accident, at his or her current and past family physicians' offices, at his or her current and past dentists' offices, and so on, which reflects the current situation in most parts of the world.

The idea of a single, unique, Internet-accessible EHR has been mentioned many times in the literature, sometimes under the name of Lifetime Health Record or Personal Health Records but none of the articles discuss the requirement of such systems beyond confidentiality [3,4,6-8]. In this article we will discuss the requirements of such an EHR system on a conceptual level, with no regard for technologies, policies, or laws for implementing these requirements.

In this article, besides EHR and EPR we will use the term *health professional* (HP), which includes all sorts of professionals who can have access to the patient's EHR, including physicians, nurses, dentists, psychologists, and alternative medicine practitioners. We will also use the term *health organization* (HO), 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 whole health history are available to the HP to aid in diagnosis, therapy planning, and patient care. This aid can take three main forms: provision of essential patient health information, efficiency through reuse of previous laboratory exams, and opportunistic improvements in quality. We will discuss these three forms of aid shortly.

Furthermore, the EHR serves as the record of an HP's actions on behalf of that patient and should be the unique and definitive source of information about 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 EHRs of his or her patients should be the definitive source of information.

The article is organized as follows: In "General Principles" we discuss confidentiality, control, integrity, and legal value and the goals of an EHR. It is important to point out that the general principles of confidentiality and integrity are well known and well discussed in the literature, but we think it is important to list them with other, less well-known and less discussed principles for the sake of completeness. In the next three sections we discuss the subprinciples related to integrity, confidentiality and control, and the legal value of the EHR. In "Other Practical Considerations" we discuss other principles of a more practical nature, which we believe are also very important. In "Related Research" we discuss some of the literature on these issues, and in the final section we discuss some open issues. This article does not propose any technical or legal solutions to the principles proposed. If

*Address correspondence to this author at the Institute of Computing, University of Campinas, Caixa Postal 6176, 13083-970 Campinas - SP, Brazil. E-mail: wainer@ic.unicamp.br

1874-4311/08

these principles are accepted, it will be as a result of the efforts of many researchers and research programs.

GENERAL PRINCIPLES

We assume the following general 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 or her records. A patient may grant access to an HP and revoke such access rights when the treatment is over.
- **Integrity:** The patient's life may depend on the data contained in the records, and therefore 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 HPs on behalf of that patient and should be the definitive source of information about said actions.

These general principles of confidentiality, control, integrity, and legal value are further elaborated and discussed in the sections that follow. The certainties expressed here will be relativized as we elaborate the ethical and practical principles.

In general terms, confidentiality and control are patient-related principles. Confidentiality allows the patient to be sure that no one but authorized people can read his or her records, and control allows the patient to grant an HP read and write access to his or her medical records and then revoke the access when he or she decides the HP should have no longer access to it.

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

Finally, legal value is a very important aspect of the EHR, not a secondary aspect, as is sometimes assumed. The EHR should be the definitive source of information about the HP's actions on behalf of the patient.

USES OF THE EHR

Medical records, especially paper-based records, have a dual purpose: They serve as a legal document that records the HP's and the HO's actions and as a written collaboration medium between HPs (in case the patient is being treated by multiple HPs) or as a reminder tool for a single HP over time.

A central, 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 in patient treatment through the reuse of exam results.

The most important aspect of the EHR is that it records the current, relevant aspects of the patient's health, including: current diseases, current complaints, allergies and other health conditions, and medications being taken. The current health aspects of the EHR improve the quality of the patient care by helping the HP to avoid drug interaction problems, recognize iatrogenic symptoms, avoid allergic reactions to drugs, and so on.

Furthermore, the EHR contains all recent laboratory exams of the patient. If the patient had a recent blood sugar test that showed normal sugar levels, as long as those results are recent enough that they are still valid, and the HP trusts the laboratory that 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, if all blood sugar measures of the patient are in a single place, an HP may notice a blood sugar pattern that may indicate a potential problem, or the HP may better interpret the results of a recent blood sugar test in the light of all the previous tests. Or the HP may determine that a current complaint might be attributed to the long-term consequences of a disease the patient believes was cured long ago. Thus, the HP's decision-making ability can be improved through the opportunistic use of information stored in a patient's medical history.

Comparison with EPRs

An EPR is a more localized medical record, kept in electronic form. It is usually controlled or owned by an HO, and its purpose is similar to that of the paper-based medical record: as a legal document and a collaboration and reminder tool.

The literature on EPR focuses mainly on confidentiality. A PubMed search in February 2007 for the phrase "Medical Records Systems, Computerized" with the keyword "Confidentiality" returned 1408 references, with the keyword "Privacy", returned 758 references, whereas the keywords "Availability" and "Integrity" returned 181 and 114 references respectively.

Integrity is assumed to be a responsibility of the owner of the records and thus a somewhat obvious requirement. Confidentiality, as discussed earlier, is a requirement that serves the patient, not the HO, and therefore must be imposed by legislation or other external constraints.

Control is an irrelevant issue in EPRs: if the patient chooses a particular HO he or she is implicitly giving this HO the right to create and manage his or her EPR. But it is very unclear how a patient would revoke the HO right to hold and access his or her records - can the patient request his or her records? Can or should the HO keep a copy of said records in case the patient sues the HO?

We are not aware of much discussion of the legal value of the EPR. Clearly all HOs are aware of the legal aspects of the records, especially requirements such as compliance with national regulations regarding the storage of records. But beyond the legal requirements for storage of records, we do not know of discussions regarding the effects of the legal value of EPR on the systems requirements.

REQUIREMENTS FOR AN EHR

Integrity Issues

As mentioned earlier, 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 oppor-

tunistic gain in quality. But in order to use the information, the HP must trust that the information is correct, complete, and up to date.

The general principle of integrity is that no unauthorized person 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. All care in making the system robust and redundant is necessary.

Principle 2: **Up-to-Datedness.** The EHR must contain all the latest relevant information about the patient's health, so there should be no significant delay between 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 that if the patient consults another HP for some other reason, that information is available.

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 the patient's records to see that he or she has an allergy to Novocaine that was diagnosed 15 years ago during a dental 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 to enable the HP to look for specific data in the patient's record.

Confidentiality and Control Issues

Confidentiality states that the patient may expect that no unauthorized party will be able to read his or her medical records. Therefore, the storage and transmission of the EHR should be guarded by security measures that prevent eavesdropping.

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

This raises the interesting question of when a treatment is over. In the case of hospitalizations, there are activities that mark the end of the treatment, but in other cases it is not so clear. Of course, the patient may decide that the treatment is over because he or she 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 or her EHR without attending the HP's office.

Another partial alternative is to grant access only during a consultation. That would preclude the HP accessing exam results that are entered into the EHR by a laboratory just after the consultation. It would also preclude the HP from discussing the case with a colleague, and so on.

Principle 4: **No Automatic Access Rights to the Patient.** The patient has no automatic right to read or change the EHR. The HP may delegate to the patient the right to read part of his own medical record, but such decision is a medical decision, one to which the HP may be ethically and professionally held accountable. This is a controversial principle that goes against the usually accepted requirements of electronic medical records and the usual understanding of ownership of the patient' medical record. To our understanding, the patient has only control over his own records, that is he or she can decide which HP can access it. But the patient cannot read and cannot change his own records, but he or she may receive a delegation to read it by one of the HP who have access to it.

Our view is that: a) the EHR is a communication medium between HPs b) it may or may not be appropriate for the patient to have access to this communication, c) it is the HP's responsibility to decide whether the patient should have read access to his EHR, and d) it is never appropriate for the patient to change the data in the EHR.

The point a) above is the whole purpose of an EHR - the communication among the different HPs caring for a patient. As for point b) we believe that granting the patient only the right to read his or her records also may pose some problems. Should a patient with a fragile physique be able to read that his doctor is considering a serious, degenerative disease as a diagnostic hypothesis? Should a patient read in her records that she is taking a placebo for her psychosomatic complaints? We believe that it is the HP's ethical and professional responsibility to choose what and how to inform his or her patients. Some professionals may choose to disclose all, some may not, but it is the HP's professional responsibility to make that choice. This is our point c) above.

We do not dispute that in most cases it is probably beneficial to the patient to have read access to his or her own records, but that is a **medical decision** of the HP, for which he or she should answer ethically, professionally, and legally, and therefore patient read access and write access **are not** a design requirement. In fact, the design requirement is not to allow read access to the patient, but allow the HP to grant such access in cases he or she feels it is in the patients interest.

Finally as for point d), we believe that any write access to the patient to change the EHR violates integrity and thus invalidates the whole purpose of the EHR. For example, can a patient with Munchausen syndrome ("the repeated fabrication of physical illness - usually acute, dramatic, and convincing - by a person who wanders from hospital to hospital for treatment" [10]) be trusted to correct his or her own records for completeness and relevance?

Our view, for example, violates the Principle of Access in the IMIA Code of Ethics for Health Information Professionals:

> *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* [9].

We believe that the right to correct the records, as stated in the IMIA's Principle of Access, is misguided and violates both the legal value and especially the integrity requirements of the record. Access for the patient to alter his own EHR, if allowed must follow the principle of incrementability below (principle 8).

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

Principle 6: **Implicit Acceptance of HO Structure.** By granting access to his or her EHR to an HO or HP, the patient implicitly accepts whatever access delegations are in place in the HO or whatever access delegations the HP defines. The HO and the HP may be criticized or punished for these delegations after the fact, but the patient cannot control who within the HO will have access, or what kind of access, to his or her EHR.

Principle 7: **Limited Read Access for Public Health, Legal, and Professional Entities.** Some legal, public health, or professional bodies may have limited and anonymized read access to the EHR without the patient's approval.

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

Legal Value

As discussed earlier, any medical record has a dual purpose: as the record of the patient's data and the record of the doctor's medical actions. The legal value of the EHR concerns this second aspect: When challenged in a legal context, the doctor must be able to use parts of the EHR to justify his or her decisions and actions. Thus, in the proper legal context it should be possible to access a particular doctor's medical actions as recorded in the patient's EHR, 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 must be a mechanism to add corrections to the information already present. When presented to an HP, the record will show only the corrected version of the data, but as we will discuss later, the uncorrected version must be kept, along with the correction, who made it, and when.

Principle 9: **Nonrepudiability.** One cannot deny making an entry in a patient's EHR. This is an important requirement for preserving the legal value of a record: If the record states that an HP decided on a particular therapy or made a particular diagnosis, the HP cannot deny that record.

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

Principle 11: **Recoverability of Specific Moments.** In order to verify the quality of an HP's 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. Therefore, the system must be able to show a snapshot of the EHR at that time, without the corrections and data entered after that moment.

Other Practical Considerations

Principle 12: **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 that reflects their actions even if they no longer have access rights to the record.

HPs and HOs have legitimate use for information about the medical actions they undertook on behalf of a patient, including: billing, research, and quality control. The HP and HO should be able to extract the appropriate segments that reflect their actions from the patient's EHR instead of keeping a second or third record for these purposes.

Unfortunately, the three legitimate uses of patient information just listed have different requirements regarding the content of the EHR. The research and quality control copies should be anonymized but should contain enough previous information about the patient from which one can judge the quality of the actions performed or at least consider 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 because that would disclose too much information about the patient.

Principle 13: **Very long storage times.** The EHR must last at least as long as the patient's life and probably longer if there are questions about the patient's death or final years. This imposes important constraints on the storage of the data: The data must be readable even after decades of storage. But, more relevant to this article, the digital signatures must also remain valid for the corresponding period so that data entered and digitally signed can be verified decades afterward.

Principle 14: **Substitutability of passwords and keys.** It is unreasonable to think that a patient will remember his or her EHR password or keep a

smart card throughout his or her life. There must be a mechanism to generate new passwords or keys for a patient (provided his or her identity has been established with the appropriate certainty). Even if the identification mechanism is based on biometric data, some biometric data may change with time.

RELATED RESEARCH

An article by Buckovich *et al*. [11], which expresses concerns similar to ours, lists 28 principles regarding electronic medical records, compiled from 10 policy documents and from U.S. organizations (such as the National Research Council), and makes a comparative review between the different sets of principles. Principle 12 in the article 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* [11].

This principle is particularly relevant to our work because it is part of our justification for denying access rights to patients, which in turn contradicts Principles 2, 3, and 4 (the right to access, right to a copy, and right to correct or amend one's own record) of the same article. Principle 12 is also our justification for the HO's and HP's right to a copy of the record of their own work.

An article by Ross and Lin[12] reviews the literature on the benefits of patients' read access to their own records 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 increased anxiety when psychiatric records are made available to the patients. An article by Staroselsky *et al* [13] reports on the benefits of providing read and limited write access to the patient's EHR in terms of accuracy of the data and compliance with treatments. An article by Powell *et al*. [14] presents a survey of 31 patients regarding which medical information they did not want to be placed in an EHR, which included matters of pregnancy, contraception, sexual health, and mental health. Also relevant is their finding that some patients pointed out information that they believe was incorrect about them in their medical records, but some of this information was found to be correct (i.e., it corresponded to what the physician intended to record). This finding supports our argument that the patient must not have write access to his or her own records.

To our surprise, we found that our view on not granting read access to his own health records is not contradictory to national legislations such as the USA HIPAA and UK Access to Health Records Act of 1990. For example, the HIPAA, regarding the rights of the patient to access their medical records, allows for the health care provider not to agree in releasing the information to the patient, if "a licensed health care professional, in the exercise of professional judgment, determined that it is reasonably likely that access to the required information would endanger the life or physical safety of the consumer or another person" [15]. Furthermore, HIPAA does not include psychotherapy notes as a medical document to which the patient has access. The UK Access to Health Records [16] is closer to our view: "Cases where right of access may be partially excluded (1) Access shall not be given under section 3(2) above to any part of a health record— (a) which, in the opinion of the holder of the record, would disclose– (i) information likely to cause serious harm to the physical or mental health of the patient or of any other individual; "

Verity and Nicoll [17] describe the tension between confidentiality of the EPR and the interest of public health surveillance and point out that if there are multiple EPRs for each patient, anonymization in itself would be problematic because of the duplication of data. In our proposal of a single EHR, those concerns would be less problematic.

A different approach to a single, central EHR is to have local EPRs that allow some degree of interchangeability. A number of articles discuss the need for standards for interchanging and sharing EPRs across different organizations or countries [4,18].

Other research articles discuss different technical aspects relevant to the issues in this article. Pharow and Blobel [19] discuss the issue of long-term storage and its impact on the digital signatures in the EHR. Behlen and Johnson[20] and Quantin *et al*. [21] discuss issues and techniques for the anonymization of medical records. Finally, to our knowledge Bakker [22] was the first to point out the requirement of recoverability of specific moments, but the article discusses the difficulty in implementing this requirement when the EHR is just a set of pointers (or links) to an HO's specific data and processes.

OPEN ISSUES

A large set of issues are not discussed in this article. First, we do not propose any implementation or technical solution to the security requirements herein. Such solutions certainly will involve complex cryptographic techniques, trusted central servers, operational procedures in HOs, and national-level legislation. We also do not discuss the content of the EHR nor how long the data should remain available in the EHR.

But we think that some of the ethical issues raised here warrant further discussion. One is whether the patient can ask for certain information to be private and not made available to other HPs. The patient may tell a particular HP some information because he or she trusts the HP and believes that the HP can make the appropriate use of that information on his or her behalf. But the patient may not trust the entire health system and therefore may want that information to be unavailable to other authorized HPs.

Another complex ethical issue, for which we have no solution, is the linking of different patients' records. Clearly there are many situations in which knowing the health conditions of a patient's parents or spouse will improve the patient's care. However, the spouse or parents might not grant this HP the right to access their records.

CONCLUSION

In this paper, we presented a set of principles for an EHR, a unique, centralized, electronic health record system

that goes beyond the usual requirement of privacy. We do not believe this is a complete set of requirements for such systems. But the requirements set forth in this paper already pose a considerable task to satisfy them. We do not know of any technological, legal or economic solution that satisfy these requirements.

Current attempts to implement some for of centralized record system usually fall short in some if not all of these requirements. For example, recent developments on Personal Health Record by Microsoft and Google do not satisfy integrity, and thus neither legal value. At current technology and legal infrastructure, it seems that the most one can do is to prioritize a subset of our principles that the system will follow, and accept that the other principles will not be satisfied.

If this paper does not put forth any solutions, we hope it make it clear that there many more requirements for an EHR than privacy, and that further research into the technological and legal aspects of an unique health record is needed.

REFERENCES

[1] Chandramouli R. A framework for multiple authorization types in a healthcare application system. In: 17th Annual Computer Security Applications Conference (ACSAC '01). Washington (DC): IEEE Computer Society 2001; 137.

[2] Blobel B, Pharow P, Spiegel V, Engel K, Engelbrecht R. Securing interoperability between chip card based medical information systems and health networks. Int J Med Inform 2001 ; 64(2-3): 401-15.

[3] Bernstein K, Bruun-Rasmussen M, Vingtoft S, Andersen SK, Nøhr C. Modelling and implementing electronic health records in Denmark. Int J Med Inform 2005; 74(2-4): 213-20.

[4] Mohan J, Razali Raja Yaacob R. The Malaysian Telehealth Flagship Application: a national approach to health data protection and utilisation and consumer rights. Int J Med Inform 2004 ; 73(3): 217–27.

[5] Blobel B. Authorisation and access control for electronic health record systems. Int J Med Inform 2004; 73(3): 251-7.

[6] Beun JG. Electronic healthcare record; a way to empower the patient. Int J Med Inform 2003; 69(2-3): 191-6.

[7] Kim MI, Johnson KB. Personal health records: evaluation of functionality and utility. J Am Med Inform Assoc 2002; 9(2): 171-80.

[8] Iakovidis I. Towards a health telematics infrastructure in the European Union. Stud Health Technol Inform 2000; 76: 23-33.

[9] IMIA. International Medical Informatics Association code of ethics for health information professionals. http: //www.imia.org/English_code_of_ethics.html (accessed November 2007)

[10] Beers MH, Berkow R, editors. Psychiatry in medicine. In: The Merck manual of diagnosis and therapy. 17th ed. Whitehouse Station (NJ): Merck and Co., Inc.; 2005. ch. 185.

[11] Buckovich SA, Rippen HE, Rozen MJ. Driving toward guiding principles: a goal for privacy, confidentiality, and security of health information. J Am Med Inform Assoc 1999; 6(2): 122-33.

[12] Ross SE, Lin CT. The effects of promoting patient access to medical records: a review. J Am Med Inform Assoc 2003; 10(3): 294.

[13] Staroselsky M, Volk LA, Tsurikova R, *et al*. Improving electronic health record (EHR) accuracy and increasing compliance with health maintenance clinical guidelines through patient access and input. Int J Med Inform 2006; 75(10-11): 693-700.

[14] Powell J, Fitton R, Fitton C. Sharing electronic health records: the patient view. Inform Prim Care 2006; 14(1): 55-7

[15] Sonya Schartz. Rights to Access Medical Records Under the HIPAA Privacy Regulation. Health Assistance Partnership. Washington, DC. 2003. (available at http: //www.hapnetwork.org/medicare/HIPAA_Resource_Center.html - accessed November 2007)

[16] Office of Public Sector Information. Access to Health Record Act 1990 (c. 23). (available at http: //www.opsi.gov.uk/acts/acts1990/ukpga_19900023_en_1#pb2-l1g3 - accessed November 2007)

[17] Verity C, Nicoll A. Consent, confidentiality, and the threat to public health surveillance. BMJ 2002; 324(7347): 1210-3.

[18] Espinosa AL. Availability of health data: requirements and solutions. Int J Med Inform 1998 ; 49(1): 97-104.

[19] Pharow P, Blobel B. Electronic signatures for long-lasting storage purposes in electronic archives. Int J Med Inform 2005; 74(2-4): 279-87.

[20] Behlen FM, Johnson SB. Multicenter patient records research: security policies and tools. J Am Med Inform Assoc 1999; 6(6): 435-43.

[21] Quantin C, Allaert FA, Dusserre L. Anonymous statistical methods versus cryptographic methods in epidemiology. Int J Med Inform 2000; 60(2): 177-83.

[22] Bakker A. Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. Int J Med Inform 2004; 73(3): 267-70.

Received: September 15, 2008 Revised: October 20, 2008 Accepted: December 1, 2008