International Journal of Medical Informatics (2004) **73**, 325—331

ELSEVIER

International Journal of Medical Informatics

www.intl.elsevierhealth.com/journals/ijmi

Digest of the discussion group sessions

A. Bakker

Addabit BV, Atjehweg 10, AP Noordwijk 2202, The Netherlands

KEYWORDS
Discussion group sessions;
Conclusions;
Recommendations

Summary In this chapter the main issues discussed at the IMIA working conference ''Realising Security of the Electronic Health Record (EHR) ''31 May—3 June, Varenna Italy are presented together with conclusions and recommendations. In total there were eight discussion group sessions.

1. Introduction

The conference was composed of four blocks each consisting of a plenary session where four papers were presented followed by in-depth discussions in two groups. In addition to these blocks there was an opening session with as keynote speaker Dr. A. Jai Mohan from Malaysia. This chapter is structured according to the subjects of the four blocks. Some issues came back in the discussion for more than one block. In this chapter such issues are dealt with in only one section.

Reports of the discussion group sessions were given/sent to the participants asking them for comments. A draft of this chapter was sent to all participants too, asking for their comments within 2 weeks time. The comments received were processed and an updated draft was sent to the participants for a final check.

2. Ethics and legal issues and patients' rights

2.1. Rights, duties, obligations of patients and healthcare professionals

Despite the fact that ICT is a common tool in health care, at least in the industrialised countries, it was felt that there is still a lot of uncertainty as to rights, duties, obligations, possibilities etc. of both patients and users. There is a need for clarification. Such clarification would facilitate more focus in the discussions and the policies to be implemented.

There is still no consensus on the rights of patients. This will be further complicated with the advent of distributed systems. In his presentation Francois Allaert advocated filtering information before giving it to the patient. It was observed that filtering would become rather complicated for a distributed EHR.

Human rights in respect of healthcare are universally applicable:

- as evidenced by the Universal Declaration of Human Rights to which 119 countries have committed;
- through logical consequences of the intent of health care to help the patient;
- inherent in the notion of a right (which the possessor has the option to exercise) is the right to choice which in turn leads to a right to information (and hence the right to access to their healthcare record).

There are very few reasons for a patient *not* to have access to their record:

- data that identifies a third party without their consent and by consequence may harm the privacy of that third party,
- data that is likely to cause *serious* harm to the patient or others were it disclosed.

1386-5056/$ — see front matter
doi:10.1016/j.ijmedinf.2003.12.010

Care may need to be taken when records are shared with the patient-breaking bad news such as the diagnosis and prognosis of cancer may require gradual, sensitive disclosure under the control of the attending clinician. However, this would be a matter of timing the information flow rather than of withholding it; the fact that a patient has made a Subject Access Request indicates, at least, a serious wish to know on the part of the patient.

The safe and secure transfer of health records is a duty of health care professionals.

Health record data should never be deleted if these might have been used in the clinical process. However, erroneous data should be blocked and thus it may be necessary to conceal such data from subsequent users except where the knowledge of the previously recorded erroneous data might affect current treatment.

Aggregation of personal health data into national data sets causes tension between privacy and public interests. To be able to deliver high quality health care services such aggregation is sometimes necessary. In such case duly qualified individuals bound to secrecy should get access under strict rules. The level of sharing and disclosure society is prepared to accept varies. In 'developing' countries with higher incidence of infectious diseases and limited budgets for health care there may be greater willingness to share than in more 'developed' countries.

2.2. Interests of patients and health care professionals may be in conflict

Originally, the patient record was not intended for the patient, but for the care team. So, it could also contain informal remarks e.g. about the patient's personality, which were not objective, but could be useful nevertheless. Certainly in the European context, at present the patient record may only contain information that can also be accessed by the patient; the only reason for not granting this being the fact that it may be harmful to the patient or harm the privacy of a third party. In some European countries private notes (which are not communicated to anyone else) may be excluded from patient access but there are rules governing when such notes must become part of the patient record.

It was emphasised that there is a potential conflict of interests between patients and health care providers. Example: a patient has the right to ask for correction of the record, but is there an objective truth? It was pointed out, that the old information should not be deleted; it must only been made inaccessible (for 'normal' users). ISO 13606 will give rules for that. Another problem is that patients are not always in a position to exercise their rights.

2.3. Educate not only the health care professionals

An important issue is the need to educate the public on what can be expected from an EHR and how far their Personal Health Data will be shared. This should preferably take place before the person is confronted with the healthcare system in his/her role of a patient.

2.4. Consent of the patient

Many of the issues around access to the data can be effectively resolved through application of a process of informed consent as proposed by Eike Kluge. An initial informed consent could be obtained in which a 'default' policy can be agreed (including use of the data for statistical and/or scientific purposes). Subsequent obtaining of consent for additional information processing and disclosure should be incorporated into the general consenting processes of healthcare. It was emphasised that informed consent is to be preferred over implied consent.

Regarding Informed Consent it was observed that what an individual *needs* to know, may exceed what he *wants* to know or *vice versa*. Further, the subject of public health interests, in possible conflict with patient's interests, was raised. Several solutions are mentioned to resolve (part of) these conflicts, e.g. the use of reversible pseudonymisation.

Also the case of transfer of information to social care workers was discussed. The rules differ considerably between countries. Countries also differ in the extent to which they have institutionalised additional health care professionals with opportunities/rights of consultation and treatment.

One of the participants reported data about willingness of patients to grant access. In cases when the procedure is transparent and the benefit clear the percentage of (chronic) patients that agree was found to be beyond 95%. If there is a general and unclear request the rate of patients willing to grant access is rather low.

2.5. Patient medical data on cards

Some experiences were exchanged about patient data on cards; there is a consensus nowadays that a card should not be the primary residence of a repository of vital data, but may be very well used in specific cases to have e.g. emergency data easily accessible. Cards are now more generally thought of in terms of tools for access control and authentication.

3. Access control to information and authorisation management

3.1. Questions about access control

Before implementing access control mechanisms a number of questions have to be answered.

1. What is the purpose of such control? Is it for:
   (a) the patient (subject of the record);
   (b) the health care professional;
   (c) the administration.
   It was agreed that the whole question of control is unsolvable unless the purpose is clear.
2. Should access control be handled differently for different types of records? E.g.
   (a) life-long records;
   (b) centralised records;
   (c) distributed records;
   (d) partial records;
   and if such differential control is appropriate, how should it be implemented in light of pragmatic constraints?
3. Who should have control and when?
   (a) the subject of the record?
   (b) the health care professional?
   (c) the institution?
   (d) the government?
4. What should the control mechanism be like? Should it be:
   (a) a feature of the record?
   (b) a feature of the access protocols?
   (c) a combination of both?
   (d) something entirely different?
   It was generally agreed that in any case, emergency override mechanisms should be integral to any form of access control mechanism (where this override function has to be defined very carefully and routinely audited and monitored). It was reported that there are several practical solutions operational where in an (initially) automatic audit process is checked whether there really was an emergency situation. If this cannot be verified automatically then an official (e.g. chief medical records officer) checks manually, with penalties for misuse. Of course it can be checked only after the event.
   It was stipulated that one could define in the Security Policy that certain categories of data can not be accessed through the emergency procedure.
5. What should control cover? (How far should it extend?)
   There appeared to be general agreement that while the subject of the record has a right of control, this right is limited by:
   (a) legitimate societal needs (planning, epidemiology);
   (b) threat of serious harm to third parties;
   (c) the ability of the health care professional to carry out consented-to health care.

It was also agreed that any access—and any imposition of access control requires robust authentication measures. It was felt that this was especially important for inter-institutional access, inter-jurisdictional access, Internet access, etc. The question of managing intra—as opposed to inter-institutional access was also raised in quite general terms.

3.2. The time-machine in the EHR

The majority of the group was of the opinion that we need the facility to reproduce the EHR as it would have presented itself to a specified health care professional at a specified point in time in the past, this to be able to interpret the behaviour of the health care professional. Not only for legal reasons, but for any situation where this behaviour has to be evaluated. It was observed that such reconstruction of the EHR not necessarily needs to be immediate because the facility does not directly affect the care process.

Some members had some doubt as to the need:

- Do we need all the data of the EHR?
- Although we need it in principle, is it worth the effort?

The technical difficulties in the implementation were perceived differently. If all data are time-stamped and a trail is kept, some members expect the implementation to be rather straightforward as long as the EHR is restricted to one health care establishment. For distributed EHR's the effort would become substantial.

It was observed that it will probably be impossible to retrofit the facility in existing (legacy) systems.

The discussion made clear that there are large differences between countries in the periods (paper) records have to be kept. It was also observed that clinical data often loose their relevance rapidly, be it that there are significant differences between different data types. Probably it will be sufficient if we can look back several years. The techniques of long term storage of Personal Health Data on different computing platforms have still not had time to be fully evaluated.

It was concluded that IMIA should be alerted to this issue and, if they recognise it as important, should take steps to explore whether the need for this facility is recognised also by other professions.

For that purpose a clear concise description of the issue is needed.

3.3. Concepts, definitions and modelling

It was felt that it is very difficult to get an overview of what is going on in the field of modelling and standardisation. The bodies involved should pay more attention to clarify their position, their results and their work in progress and correspondingly IMIA should actively attempt to participate more extensively in these standardisation activities.

There is a danger that the gap between their activities and the implementation of EHR systems becomes wider and deeper.

It was mentioned that several modelling activities, like openEHR, try to pay attention to these aspects already, their efforts should be encouraged.

The UMLS modelling deals only with the medical domain, no attention is given to legal, informational and technical aspects.

A complication in modelling is that the concept definitions are rather dynamic than static, they evolve over time. A static model soon becomes out of date.

3.4. Integrating pieces of information from different information systems is still an issue

It was agreed that a distributed EHR requires a register containing references for each patient to places where his/her medical data could be found. It was observed that such register could not be avoided by implementing a system with for each patient a smart card containing these references because:

- the patient will not always be present when the data are needed;
- the patient will not always have the smart card available;
- a back-up system for the cards would be required.

3.5. A comprehensive model of the EHR

A comprehensive model of the EHR would be quite helpful, but we should realise that it is a huge and never-ending activity to develop and maintain such model. The number of concepts may be estimated from systems managing medical ontology such as SNOMED and UMLS. These systems are still growing from currently about 280,000 concepts to probably about 400,000. Until now only a few hundred concepts are modelled in OpenEHR. Unless this process is accelerated dramatically the results will be of limited value for EHR developments in the coming 5 years.

It was recommended that IMIA become more active in the modelling domain and works together with other professional associations and bodies (e.g. WHO), to stimulate transparency and coherence of the modelling activities.

3.6. Implementation of access rights and authorisation management

The group felt that case descriptions of implementation of access control and authorisation management would be quite useful. A problem is how the effort involved could be rewarded. It was recommended that IMIA stimulate the development of such case descriptions and makes these accessible through the IMIA website.

4. Secure systems architectures for the EHR and health information systems

4.1. The composition of the EHR

It was emphasised that the EHR is more than the collection of what data (observations) are available about a certain patient (in the information systems of the health care establishments the patient has been in contact with), this is only part of one pillar: the knowledge. The other pillar is formed by the actions (to be) carried out. The interpretation being the bridge in this model.

4.2. Does the patient own his/her record?

The question of ownership was discussed, and the following points emerged:

- The concept of ownership in general encompasses several distinct rights that are best captured by the notion *of dispositionary power*. In the case of EHRs, these include:
  - the right to control access;
  - the right to sell for a valuable consideration;
  - the right to determine usage.
- It was agreed that the patient has a dispositionary power over his/her health care record and that:
  - this may have financial implications, especially with respect to DNA information that may be contained in the EHR, but that;
  - diagnostic algorithms, etc. contained in the EHR do not belong to the patient but to the originator of the EHR.

- It was further agreed that while the patient has a primary dispositionary power over her/his EHR, the material instrument in which the EHR is recorded remains the property of the originating agency.
- It was also agreed that:
  - clinicians (and institutions) have a right to access the EHR for all purposes related to the fulfillment of their professional duties;
  - therefore the control exercised by the subject of the EHR should not interfere with the ability of clinicians (and institutions) to meet their professional duties;
  - clinicians have right to access relevant EHRs for the purpose of self-defense.
- Finally, it was acknowledged that if the subject of an EHR is a member of a recognized ethnic or other collectivity, the latter may have a share in the dispositionary power over the record. The implication of this for access control must be explored.

4.3. Quality and ordering of services, contractual relationships, customer relationships

- There is a need to keep in mind that our results should be globally useable; this will not be possible for (all) solutions, but should hold for all principles. It was observed, that in our discussions, the focus is almost always on our own setting, without taking into account the global context.
- Again a definition problem was mentioned: what do we see as our principles?
- A risk based approach was advocated and *this is indeed mandated in Article 17 of the European Data Protection Directive*. Ensure to have sufficient evidence to measure effectiveness. Clinical Incident Reporting Schemes (on a wide base, broader than just one institution) should be in place, with a strong emphasis on the need to realise that in a no-blame culture we try to learn from errors. Not many such systems are in place, but this line should be supported. This wider requirement is in addition to the requirement for Security Incident Reporting Schemes, although they will overlap partly.
- Definition of responsibilities seems also to be a significant problem in many places. Clarity is needed also there.
- Important question: can we bridge between the developments in the different countries, and try to avoid ending up with many incompatible systems?
- In relation to the previous item: how important is it really, because as yet there is not much cross-border flow of data (although some counter-examples are given). This may change, however, since there seems to be a recent EU decision, that patients have the right to apply for healthcare services anywhere within the Union.
- A common European Health Policy is clearly missed. No initiatives on this subject are known.

4.4. Practicality and planning

- Not everywhere a database manager (i.e. a responsible official) for hospital patient data has been appointed (yet?).
- Sometimes significant progress can be achieved by starting small scale, without thorough planning beforehand (see example in Rod Neame's lecture).
- There is a need for a better definition of the health information professional. This could go hand in hand with a better positioning in general of medical informatics. In this respect, a link with the IMIA working group on education is important. It is also a part of information governance (see lecture of Alistair Donaldson). Although several groups are addressing this idea of core competencies IMIA should not remain passive [see for instance the UK CHIP activity which seeks to develop registration arrangements for health information professionals, http://www.ukchip.org).

4.5. Without an international authority how can international rules be agreed and enforced?

- Complex sharing rules require political force to implement.
- There are possible roles for Council of Europe or OECD.
- However, requirements must accommodate models other than nationally coordinated healthcare delivery, such as those based primarily on insurance.
- In many parts of the world the incentive to develop controls will be driven by health care insurers—the liability (and financial impact) arising from inadequate security in shared health records should therefore be explored in conjunction with insurers.
- International travel operators are also influential in healthcare improvement since they wish to sustain travel to all countries and therefore to reduce personal risk for travellers, in our case

the risks associated with insecure health records management.
- IMIA Security Working Group should draft recommendations on controls and procedures appropriate to transfer of health records [CEN251 WGIII and ISO TC215 WG4 have draft standards going through the processes of adoption in exactly this area, http://www.centc251.org and http://www.iso.org/iso/en/stdsdevelopment].
- *Health Informatics*—International transfer of personal health data covered by the EU data protection directive—High level security policy WI NEW (DPCGUIDE).
- *Health Informatics*—Data Protection Contract Guidance WI 150 (POLINTRANS).
- *ISO/DIS 22857 Health Informatics*—Guidelines on data protection to facilitate trans-border flows of personal health information.
- Inter-organisational sharing of records requires more than contract-based registration and authentication.
- Strength of authentication relates to the strength of registration.
- End-to-end encryption of data is preferable to point-to-point schemes (such as SSL) which give a false sense of security.

4.6. Who governs information governors?

Information governors may be governed by:

- statutory regulation;
- accreditation of organisations;
- certification of applications.

Countries vary in their approach, using one or more of the above, and in the scope of application (e.g. in Italy accreditation is applicable only to hospitals delivering care in the public sector). Nevertheless, it is a clear requirement that governance is in place and that people have responsibilities for addressing the various facets of that governance. The European Data Protection Directive establishes Supervisory Authorities and Judicial Remedies for breaches of its requirements.

4.7. What can be done about duplication of entries in master patient indices?

There was a consensus that a secure distributed EHR requires a unique patient identifier on a national scale. Implementation of such a unique identifier may solve the problem of duplication in master indices. In some countries a national unique identifier is forbidden by law. It was felt that for a fruitful development of the EHR such laws should be adapted to at least allowing a health care specific unique identifier.

In several countries an identifier used in healthcare should not be used in other sectors (the Canadian Provincial healthcare identifier may not be used in other sector records). The use of National identifiers created for purposes other than health care (e.g. a national security number) has serious disadvantages and is prohibited in several countries.

If cross-sector linkage is to be allowed at all, it should only be allowed following approval of a national Data Protection Commissioner (as in Greece).

5. Ensuring the security of web-based systems and coping with mobile users

5.1. Authentication

Preferably authentication of users should always use at least two factors, each being from the different silos: ''Something you know'', ''Something you are'', and ''Something you have''. Authentication may use multiple factors from certain of the silos mentioned above, in order to replace a single factor from another silo.

Care needs to be taken in deploying authentication schemes, that delivery of patient care is not hampered. For that reason special attention should be paid to emergency situations.

The requirements level for authentication will depend on the application. For health care dealing with ''lifestyle threatening data'' we can often expect the highest level to be required. Differing levels of system privileges may be allocated depending on the level of authentication achieved.

The widely applied authentication with a personal (secret) password is inadequate although it can be improved by the adoption of good password management such as established in ENV12551 Health Informatics—Secure User Identification for Healthcare-Identification and Authentication by Passwords—Management and Security.

There is cultural resistance to adopting multi factor authentication in some jurisdictions.

5.2. PKI

Despite the fact that we have seen a slow introduction until now and the costs are still rather high, there was consensus that PKI will become the major tool for ensuring security of the EHR As strong arguments were mentioned:

- the banking sector is committed;
- commitment of the German patient card.

The certification authority will probably be organised hierarchically with as an extreme the UK with the root certification authority in the NHS. Anyhow interoperability is required.

It was emphasised that PKI is a tool with a wider applicability than just healthcare.

5.3. Biometrics and genetic identification

It was emphasised that biometry is still developing. At this stage it can be a useful technique for verification. For identification it will be applicable only in small populations (this due to issues of sensitivity and specificity). In some cultures resistance to adopt biometric authentication can be expected.

The use of genetic identification was judged to be unethical and also unrealistic.

5.4. Certification of parties and components

The answer to the question who should certify depends basically on whom you trust. In Germany we find two bodies on a national level:

- one that certifies devices and software;,
- the other for the accreditation of TTP service providers.

It was considered the responsibility of the government to create a trustworthy structure for such certification.

5.5. Standardisation of security policies

At the preceding working conference (Victoria 2000) it was recommended to develop a high level security policy framework, this to facilitate exchange of patient data between health care institutions and to stimulate adequate policy bridging. In the meantime it has been experienced that it is not easy to develop such framework. The working group is aiming now at a short document based on the Code of Ethics for Health Information Professionals (as adopted by the GA of IMIA), giving some guidance for the daily practise.

In this conference it was observed that a range of standardisation activities is going on, the risk was recognised of a diversity of standards that are not fully compatible.

Although the government might help by supplying templates it was judged unrealistic to expect that a common policy for healthcare can be found. The definition of common concepts was seen as a better approach.

5.6. Case descriptions

The case descriptions presented were judged to be quite valuable, more of such descriptions would be appreciated. A formal framework for such descriptions was considered to be too rigid in this rapidly evolving security domain. Fully free format on the other hand would make it difficult to interpret and compare cases. As a compromise it was suggested that the IMIA Security working group would develop and maintain a list of aspects that at least should be addressed in the case description.

A useful Australian initiative was mentioned about having an annual conference, where the real course of projects is being reported, complete with successes and failures (Third International Conference on Successes and Failures in Telehealth (SFT) 25–26 August 2003, Brisbane, Australia, http://www.coh.uq.edu.au/coh/conference/sft/2003/2003Advert.htm).

6. Some general comments made

It was emphasised that 100% security can not be realised. Education and awareness are at least as important to achieve an acceptable security as the techniques to be used.

The implementation of security measures should be based on a risk assessment.

The concept of better health care through deployment of technologically enabled services has the potential for placing barriers between the ''haves'' and ''have nots''.

Acknowledgements

The content of this chapter is largely based on the reports of the discussion group sessions by: Nick Gaunt, Eike Kluge, Kees Louwerse and Andy Truscott, because their reports were clearly structured it was no heavy task to produce this chapter.