A. R. Bakker

BAZIS Foundation
Leiden, The Netherlands

Review Article

Security in Medical Information Systems

Abstract

This review article addresses security in medical information systems. First, it is discussed why special attention is necessary for security in this field. Next, the history is considered, together with the role of IMIA. Current research issues are presented. The ongoing activities in the AIM SEISMED project are briefly described, followed by a consideration of standardization. The article concludes with an appeal to pay more attention to the security aspects of information systems.

Keywords

Medical Information Systems; Security; Confidentiality; Availability; Data Protection.

1. Introduction

Unfortunately, the terminology used in the field of 'security', 'safety' and 'data protection' is far from uniform and even confusing. This was observed already by the IFIP/IMIA Working Group 4.4 (later named IMIA WG 4). They proposed to distinguish two different aspects [1]: usage integrity and data/program integrity. Later 'availability' was recognized to be another dimension. It seems that the discussion on terminology and contents of the field is now converging on a definition of three axes that are not orthogonal: (1) confidentiality; the prevention of the unauthorized disclosure of information; (2) integrity; the prevention of unauthorized modification of information; and (3) availability; the prevention of the unauthorized withholding of information or resources. The definitions are taken from the ITSEC report [2].

When considering the definition of integrity one should bear in mind that computer programs are a special type of information. The security of any health information system will be threatened by both external and internal factors that may affect each of the three axes mentioned. Measures can be implemented to affect these threats and in that way reduce the risk. One should realize that, although the risk can be reduced by implementing measures, it can never be eliminated completely. The selection of measures to be implemented, implies balancing of risks and costs. In this process the effects to be expected of candidate measures should be assessed. Apart from direct costs, the organizational side-effects of measures should also be taken into account, the systems should remain 'usable'.

In Section 2 it is first discussed why special attention is needed for security in health information systems. In Section 3 some attention is paid to the history of security in our field and to present issues. Paragraph 4 gives a short description of the AIM SEISMED project, a major European project in this field; and Section 5 deals with standardization.

2. Security in Health Information Systems, What is Special?

One might wonder in what respects security in health information systems is different from that of other systems where identified data on people are being recorded. The following aspects can be mentioned:

- health information systemsoften store identified data on the health status of people; such data are often highly sensitive and should be treated as confidential;

- specific selections of these confidential data are needed by many health care professionals for their routine task. So, access control and authorization deserve special attention; a complication is the often diffuse organization of health care institutions;
- the recorded data play an essential role in health care delivery, they may even be mission-critical. So, availability and quality of the data deserve special attention, e.g., in hospitals an around-the-clock availability is required;
- since the data play an important role in the care process, the speed of processing and communication is important, so "on line transaction processing" often exists;
- the data are not only useful to support the care process of the individual patient, but also for research. Statistical analysis of data of groups of patients can provide additional medical knowledge for further improvement of health care. Here, a conflict between the right of privacy of the patient and the interest of the community appears;
- the physical environment of a health care establishment is often open. In hospitals, both patients and visitors are free to enter the premises, barely restricted by visiting hours.

None of the aspects listed above is unique for health information systems; the combination of these aspects, however, justifies special consideration. The special position of medical databanks has been recognized at an early stage, as illustrated by Recommendation R81 of the Council of Europe [3]. In various countries, in their national data protection acts, medical data are treated as a special category.

3. History and Present Issues

Although initially only potential benefits of the application of computers in health care were described, since the early 1970s the threats to privacy have also received attention [4]. IFIP-TC4 organized the first working conference on this issue in 1976 [5]. This led to the creation of WG 4.4 "Data Protection in Health Information Systems", chaired for many years by Gerd Griesser from Kiel. The working group organized two working conferences (1980 and 1983) that led to published proceedings: *Data Protection in Health Information Systems, Considerations and Guidelines* [5] and *Data Protection in Health Information Systems, Where do we Stand?* [6]. In addition, the working group organized workshops during the MEDINFO congresses. The next working conference, with the title *Caring for Health Information* will take place in November 1993 in The Netherlands. Within EFMI there is a working group on data protection that organizes workshops during MIE congresses and together with the AIM office of the EC organized a dedicated working conference, *Data Protection and Confidentiality in Health Informatics* in March 1990 [7]. The field of data security is not static, the increasing intensity of the use of information technology for an ever-increasing number of applications in health care makes questions on security more pressing, the more so when the applications are closer to direct patient care. Besides, new technologies introduce new opportunities, but also new threats that require new defensive measures. Sometimes the new technologies offer possibilities for better protection. So, there is a need for continuous attention. In the remaining part of this review the most important current issues in the field are briefly discussed.

3.1 Increasing Awareness

While the need for attention to safety when applying technology is well recognized in general, the awareness of the risks involved in the application of information technology in health care is rather limited. Only for the confidentiality issue there appears to be some interest, albeit not in a large percentage of the population, as demonstrated by the very few patients who exercise their right of inspection of the data recorded. In general, the interest of health care professionals appears to be rather low; reference can be made, in this respect, to the sloppy way passwords are handled. Users are interested, of course, in a high availability of the data. However, independent auditing of the measures taken to realize this security is very seldom, and attention paid to software quality is very low. This holds true for software produced by professional vendors or the hospital's data processing department. In software development by end-users, often quality control of the software is lacking completely. Thus, the most important issue in security is increasing the awareness that security should be taken seriously, to convince the health care community that there are real threats, that harm occurs, that appropriate measures may reduce the risks considerably, and that security measures deserve support. More sophisticated counter measures, improved legislation and more money will not have the expected effects unless we manage to increase the awareness of the necessity to protect.

3.2 Legislation

It is widely accepted now in the industrialized countries that data protection legislation is needed to guarantee the rights of citizens. After the Recommendation of the Council of Europe [3] the European countries are gradually establishing their national laws. Unfortunately, these laws are not identical. The diversity of the legislation led to the recently published

"Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data" of the European Commission [8], that is now being commented on by the member states. When accepted, the member states will be obliged to bring their national laws in line with the contents of the directive within four years. A legal issue that requires more attention is the replacement of signed paper documents by computer registrations. For medication orders, for instance, it is required by law in several countries that the prescription be on a signed piece of paper. Strict adherence to that requirement could seriously hamper the application of information systems for ordering management in health establishments.

3.3 User Identification

When a user tries to access an information system, he is requested to identify himself, usually by means of a personal password. Although this procedure has been used for many years, user identification still deserves attention. The proliferation of terminals/workstations in health care, even in patient rooms, and the introduction of applications where user identification is considered equivalent to signature, raises questions about the effectiveness of this method. On the one hand we see suggestions to improve the password system, including, for example:

- requirements concerning the passwords allowed, e.g. at least N characters, no numbers, no passwords consisting of letters only;
- requirements concerning the password management, e.g. to be changed every M months, the instants to be generated by a computer;
- measures to avoid that terminals/workstations are left unattended, e.g., by automatic log-off if the terminal is not active during a defined number of minutes. To avoid becoming the 'normal' procedure not to log-off when ending a session, it is also suggested to make the password invalid in case of automatic log-off or to generate a warning at the next log-on for this user, followed by a certain waiting time. A message can also be sent to the supervisor of the user concerned;
- asking with a defined average frequency for re-entry of the password, to check whether the identified user is really using the terminal. If not an alarm message can be sent to the system manager.

On the other hand, we see suggestions to use machine-readable tokens to identify the user, like a magnetic strip card or a smart card, possibly combined with a password system. It is also suggested to use biometric characteristics of the user, like fingerprints or voice. Accurate user identification, with a limited burden on the user, is not a specific problem for health informatics, nevertheless, the sensitivity of the data combined with a frequent shift for many users from one terminal to another (e.g., for nurses and physicians) justifies special attention. One should bear in mind that the effectivity of the user identification measures depends heavily on the attitude of the users. A personal badge will only be effective if it is kept as private as a credit card.

3.4 User Authorization/Access Rights

Although a health information system will hold a variety of data, each user should have access only to those data he is entitled to (that he needs to carry out his task). So, even if the user has a valid password and is allowed access to the system, this access should be restricted. Bearing in mind the wide variety of data recorded in the information systems of large health care establishments and the different roles of users in these organizations, one can imagine that describing the user-specific access rights is not an easy task; there is no generally accepted solution.

In this section the complexity of the issue will be underlined and some approaches will be indicated. The larger health information systems are, in general, built up of subsystems, software packages that support a certain activity/domain of the institution, e.g., a laboratory system, a radiology system, a meal-supply system, a medication system, accounts receivable, etc. The access of users to the data in the databank is through such subsystems. Within each subsystem a number of functions can be identified. Each user is granted the right to use some explicitly listed subsystems. In general, within a subsystem a number of functions can be distinguished; when granting access to a user, the functions he will be allowed to use are again listed explicitly. Since some functions can operate on different types of data it has to be described in addition to which data categories (files, records, fields) each user has access and what is the type of access right (read, write, modify, delete). For a typical hospital information system it becomes very difficult to define the rights for each user separately. So, it is suggested to define user roles, where a certain role leads to a set of access rights, e.g., the role of a laboratory technician at the clinical chemistry laboratory, a receptionist at an outpatient clinic, or a clerk at the invoicing department. When doing so, it is found that the role description should be parameter driven (a typical parameter being the department the user is working in). It is also found that the job name is not sufficiently specific, a secretary at some department may have more extended tasks than one at an other de-

partment. So, it is suggested to define user profiles and consider for each user which combination of profiles is applicable for his job. Because central management of user access rights is not only a significant task but may also be too far removed from the real activities, there are set-ups where granting (subsets of) access rights is distributed to heads of departments. Of course, the function to grant access should itself be subjected to specific authorization. In addition to a check whether the user has the right to use a specific function and to access certain categories of data, it is highly advisable to check also on 'the need to know'. When patient data are concerned this can be implemented by checking whether the user is involved in the care process for that patient. In an integrated HIS this can be done by checking whether the patient is admitted to the ward the user is working on, or whether the patient is on the waiting list, or was recently discharged. For outpatients the appointment system and the registration of visits can be used. In general, access should be refused if no such relation is found. However, in health care one should have provisions for emergency situations. In such situations the relation between the patient and the care provider will, in general, not yet have been recorded in the system, so there is a need to be able to override the protection. A solution [9] is to give some users (typically certain physicians and nurses) the right to state that they need the data for dealing with an emergency; the system will ask them to specify the reason (a text string), after which the access is granted. The system will report the occurrence of this event, together with the reason given to a supervisor, e.g., the medical records officer, who will check whether it really was an emergency. If not, disciplinary measures will have to be taken.

3.5 High Level Policy

It seems evident that for each information system a clear statement on the policy for the security of the system is needed. Such a statement should be issued by the management of the responsible health care institution. In practice it is found that such a statement is often missing [10] and that the existing statements show a wide variety as to subjects dealt with and the specific contents for each subject. There is a clear need for harmonization. In some countries the data protection laws require a separate regulation for medical information systems. In The Netherlands this obligation led to model regulations that describe the duties of the keeper of the data, the rights of the data subjects, the rules for supplying of data (both for the care process and for research), the policy for long-term storage, etc. The publication of a proposal for a uniform high-level policy would be of help for the management of institutions who want to take security matters seriously.

3.6 Networks and Encryption

The developments in network technology and its application in health care lead to changes in security requirements. Initially the networks were of the twisted pair star-type and restricted to the premises of the institution. The connected devices were, in general, dumb terminals. For such networks the security is, in general, restricted to password protection of the terminals. Since the risk of wiretapping is limited, usually no special measures were implemented.

As new issues in the domain of networks that arise from technological developments can be mentioned:

- networks that cross the borders of the institution, open access for users/devices outside the direct control of the institution;
- connection of computers (e.g., PCs) offers the opportunity to generate requests at a much higher rate than is possible with dumb terminals. This leads to a need to review the protection measures. For instance, rapidly repeated log-on attempts generated by a PC are a threat to break a password.
- the connected computers may request a large volume of data and build their own derived databank that can be used outside the control of the feeding information system. Even if the access to the data were legitimate, such usage requires special attention;
- when the networks are based on a backbone architecture, redundancy requires special attention;
- the risk of tapping of the messages increases, in case all messages travel on one cable;
- if the network makes use of satellite equipment rooms these should be protected;

As security services required in networks can be distinguished [11]:

- authentication of a communicating entity and the source of data - access control;
- data confidentiality;
- data integrity;
- non-repudiation, guaranteeing that a message really reached its destination.

In general, health care can make use of the achievements in network security reached in other application domains, like banking and military applications.

The level of security required in health care will, in general, be lower than in the other domains mentioned, so the issue is to make a proper selection. Besides, the organizational aspects will require special attention.

3.7 Encryption, Electronic Signatures

To protect data during transport and storage, encryption can be applied. Stimulated by the needs of other application domains, such as banking, military and diplomacy, techniques have been developed that allow for efficient encryption. Especially the key management has received attention. Special hardware chips for encryption have been developed. In practice the application of encryption is in general restricted to the password file and some types of external communication. However, the interest in encryption has increasing with the introduction of networks crossing the borders of the premises of the institution. Besides that, encryption is an important issue for electronic signatures and the authentication of messages. As stated before for networking, it is improbable that health care will need specific techniques, the requirements for other application domains are clearly higher than for health care. The issue is the selection of the techniques to be applied and the appropriate organization to make them effective.

3.8 Security in Design and Implementation

It has gradually become clear that security should not be an add-on of an information system, but rather be an integral part of the design and implementation. Even if this principle is accepted, it is not obvious what steps have to be made to achieve the expected level of security. Even after the rather dramatic effects of software/design errors in other application domains (such as the USA missile programs) health care is slow in developing a culture to take this issue serious. Errors in design, programming and implementation may lead to serious harm to the patient so that attention to this problem is strongly indicated. For introduction of new drugs most countries have a strict control system, for information systems, however, such a control system has not yet been developed. This observation holds already true for software offered by professional suppliers and software developed by the data processing departments of the institutions, where at least some attention for quality can be expected. For software developed by health care professionals themselves (often PC based) often quality aspects are overlooked completely. Also here, raising awareness is a top priority. Application of ISO 9000-3 standards may lead to development methods that give an increased chance for good quality. For systems that directly affect patient care (e.g., medication, ICU, electronic patient records) certification of the system could be required.

3.9 Availability

With the increasing role of information systems for a wide range of activities in health care institutions, also the need for high availability increases. Most of the institutions are operational 24 hours per day, seven days per week. When the information systems give direct support to the care process the systems in general will also have to be available round-the-clock. Since 100% availability cannot be realized, a procedure should be prepared for situations when the system is "down". It would be helpful if such procedures would be published, since for each system the wheel is reinvented, if invented at all. To increase availability several measures are proposed, of which some are in common use, like (partial) duplication of hardware, on-call operators and system managers, safe-copies of the databank outside the computer center, fire protection, back-up power supply, back-up computer center, written contingency plan, etc. In The Netherlands the BAZIS foundation has a mobile computer that can be used by the participating hospitals to take over the task of the hospital information system computer center within 24 hours in case of an emergency. The availability issue in health information systems is not different from that in several other application domains. The question to answer is: "what level of availability is required?" As soon as this answer is given measures can be selected and implemented to reach that level.

3.10 Smart Cards

Smart cards may be used as a carrier of patient data and also as a token that identifies the user (in combination with a pin code) describing his access rights. The first type of application raises questions as to the access rights of health care professionals to data collected in other institutions. Data present on the card are not necessarily available to health care professionals; the rules for access and the check on a relation with the health care professional deserve new attention. It is suggested to give the patient control over the access, by means of a pin code. This, however, leads to complications in case the patient is not able to execute this act of granting access (e.g., the patient is unconscious after a traffic accident). The possibility to override the access control as described in section 3.4 is more difficult to implement since there is no central controlling authority. Storing medical data on a card and making these data available to (authorized) health care professionals in other institutions requires standardization of terminology and data representation. Another issue is the completeness of the data on the card, since medical data will often be obtained while the patient (and his card) are not present, e.g., in laboratories. The patient should be legally

protected from pressure to make the data available outside the care process, e.g., by employers when he applies for a job.

3.11 Very Large Databanks

Over the years, techniques have been developed for safeguarding the databank. The basic principle is that periodically (e.g., each day) the contents of the databank is copied to a separate medium and stored in a safe place. During operation of the system all mutations on the databank are recorded on a separate medium, the logfile. In case of corruption of the databank, the most recent safe-copy is loaded and with special recovery software the mutations are processed, leading again to an up-to-date databank. Safe-copies are taken online during periods of low transactional activity (in general during the night); recovery generally takes several hours. The procedure described is successfully applied, with some refinements, for alpha-numerical databanks that typically hold several Gigabytes of data. For very large databanks for medical images (Picture Archiving and Communication Systems, PACS) this procedure cannot be used because the speed of present-day technology leads to unacceptable copy times. As an illustration: the size of a PACS databank for a 500 bed general hospital will be 1 Terabyte if a compression ratio 1:10 can be applied and the images have to be stored for a period of 10 years. With a net copy speed of 1 Mbyte per second the safe-copy process would take about 300 hours [12]. For PACS special techniques have to be developed to cope with the very large databanks.

3.12 Medical Audit

With the increasing role of information systems in health care and the gradual evolution of an electronic patient record, it can be expected that the systems will also play a role in medical audit. This will not only lead to additional requirements for the reliability of the data stored, it can also lead to the need to let the system reproduce its behavior that would have occurred at a specified moment in the past. This is to be able to judge whether the health care professional reacted at that moment in an appropriate way in view of the data that were available at that time. This is not only a technical requirement that present systems are not able to fulfil, it also may lead to a problem with the privacy rules that often state that data may only be stored for a predefined period, after which they have to be deleted. So, it may happen that data that were produced at a moment in the past cannot be reproduced since they were deleted according to the rule of limited storage periods. This issue should be further studied; perhaps a way out may be to keep the deleted data physically stored in the databank, but allow access only for the audit function. In several countries this may require an adaptation of the regulations and perhaps even of the law.

3.13 Epidemiology

The databanks of health information systems contain many data that can be used as input to epidemiological research. The key question is whether it is allowed to use the data for that purpose. Use of the data may lead to a breach of confidentiality. Even when the data are made anonymous, the risk remains that the identity of the patient concerned will appear from the actual contents of the data. In addition, the so-called "group privacy" of certain categories of patients may be at stake. Epidemiologists claim that too strict application of the protection principles may seriously harm their research, to the detriment of progress in medicine and health care. On the other hand it is argued that the principle of informed consent of the patient should be maintained and that patients in general will react positively to requests to make their data available anonymously if the purpose is explained. It appears that in this respect there are significant differences between countries, also reflected in the legislation and its application.

3.14 Selection of Measures

The issue of implementing protection measures is to defend against threats. Threats may come from outside the organization, but also from inside. Threats may be related to hardware, the environment, software, data, people, data carriers, etc. There is a wide range of measures that is proposed to improve security. Such measures may relate to the environment, hardware, software, or the procedures. Measures may improve security in two different ways, the first effect can be reducing the probability that a certain incident will occur, e.g., fire prevention. The other effect can be reducing the damage in case an incident occurs, e.g., safe-copies of the databank that together with logged mutations allow for reconstruction in case the current databank is lost. Selecting measures is a process of balancing the risks and the costs of the protection measures. In this process it is important to realize that 100% protection cannot be realized. The risk can be reduced, it can not be fully eliminated. With a threat we can associate two quantities: the probability that an incident will occur, and the size of the damage to be expected. Multiplying the two quantities gives an overall quantification of the risk, sometimes called exposure. In general, protection measures are chosen intuitively, the choice may be made be-

cause other organizations (with perhaps quite different risks) implemented them or because somebody has a personal preference (hobby horse). The risk analysis process tries to get a clear understanding of the risks for a specific information system in a specific setting and to find a balance between the costs of the measures and their effect. In view of the significant costs of protection measures it is surprising to observe that the interest in systematic risk analysis is limited until now; the selection of measures is mostly based on tradition and intuition; in this rapidly evolving field of health information systems this in itself should be recognized as a significant risk.

4. The EC AIM SEISMED Project

It is not intentded to mention in this article specific research projects that address security in health information systems. For one project, however, an exception is made: the SEISMED project (Secure Information Systems in MEDicine) that is being carried out as part of the AIM program of the European Commission. The information supplied here is derived from the project description (technical annex). The project itself describes the goal as: "The purpose of this project is to provide practically useful advice and guidance on security matters to all those in the healthcare community who are involved in the management, development, operation or maintenance of information systems, by developing a consistent and harmonized (thus transferable) framework for medical data protection throughout Europe. This framework will consist of technical guidelines and a code of ethics for health informatics". The project started in 1992 and will continue till the end of 1994. The consortium that carries out the project consists of 18 members from 9 countries, it is led by The SSADM College Limited (SCOLL), London. Among the contributing organizations we find universities, hospitals and industries. Based on a recommendation of the AIM data protection workshop in 1991 [7], the project introduces so-called "reference centers", major computer systems that will not only serve as a testground for the results of the research and development efforts of the project, but also as demonstration sites where other organizations can see the practical results. Also measures proposed by other groups might be tested here. In the technical approach to achieve the objectives of the project three main axes can be identified:

1. the identification of the needs and requirements of the medical community for data protection, as well as the recording of techniques and practices used at present.
2. the development of guidelines for enhancing security in existing healthcare information systems and for designing secure future healthcare information systems.
3. the implementation of the guidelines developed in four health care institutions in order to ensure their practical usefulness and their applicability.

It is expected that this project will have a major impact on the field. For that reason the subprojects ("workpackages" in Eurospeak) are briefly described here. Many of the current issues mentioned in Section 3 will be found amongst the workpackages of the SEISMED project, an indication that the project is addressing a significant part of real needs.

4.1 Survey

A survey will be conducted to identify current practices in and attitudes towards information systems security in health care institutions throughout EC Member States. The other workpackages contributed their individual questionnaire requirements. The results of the questionnaire serve as input to the other work packages.

4.2 Define High-Level Security Policy

The objective is to reach a common understanding of what security is and what its objectives should be in health care institutions in all EC countries and to derive a set of principles to govern medical data protection throughout EC countries.

4.3 Risk Analysis

The objective is to demonstrate the benefits of a risk analysis review by carrying it out at the reference centers. Risk analysis is expected to identify and justify an appropriate protection mechanism for health information systems. For the reference centers this workpackage is expected to yield a justified and practical set of security measures. The risk analysis is carried out by selected staff of the reference centers under supervision of external experts. A guideline on application of risk analysis for health information sysyems will be produced.

4.4 Security in System Design and Implementation

Security should not be an add-on, but an integral aspect of the design. Also during implementation, security should be considered as an essential aspect of the system. In this work package guidelines will be produced for taking security into account, both in the design and the implementation of the system. As for all other guidelines produced in the scope of the SEISMED project, the reference centers will serve as test grounds.

4.5 Security in Existing Systems

The previous workpackage will produce guidelines how to design and implement new systems. For existing systems often adaptations will be needed to achieve an acceptable level of security. The workpackage will address this issue and produce guidelines.

4.6 Encryption Guidelines

In this workpackage the requirements for an encryption service will be identified, largely based on risk analysis. The requirements will lead to specifications. The specifications will be input to the development of a working prototype in a non-operational environment.

4.7 Network Security

The objective of this workpackage is to produce guidelines for the provision and management of security in information systems networks for health care organizations. First, the requirements will be identified, mainly based on risk analysis, followed by the selection of suitable mechanisms for the provision of the required security. Next, the manner in which the mechanisms are to be used will be specified. This protocol specification will use as input the high level policy results (4.2). The reference centers will check the mechanisms and protocols on practicality. The guidelines to be produced by this workpackage will be targeted at providers of network security for distributed applications of information technology in health care.

4.8 Legal Framework

The objective of this workpackage is to develop a Health Informatics Deontology code. As a first step, the existing medical data protection legislation was analyzed for each of the Member States and Switzerland. As a next step, existing codes of international and national professional organizations of health care professionals and informaticians will be reviewed and analyzed, especially the clauses relevant to medical data protection. Based on the results of the preceding steps, a draft code will be developed that will be offered to professional organizations for comments. After processing these comments a final draft will be produced.

4.9 Results of SEISMED

From the short descriptions given here it becomes clear that SEISMED is not trying to develop new techniques for security in health information systems, but rather to produce guidelines for how existing techniques can be effectively applied. This is in line with the observation made in section 3.1 that the main problems in the field are a lack of awareness and missing clues to get security implemented in practice. The role of the reference centers in the project is crucial; on the one hand they supply input on what the actual problems are, on the other hand they are a testground for draft guidelines.

5. Standardization

At first sight one might wonder whether standardization in this field is needed. One might argue that standardization is not desirable because it might help potential intruders to attack systems by giving them more knowledge of their target. However, advantages of standardization are expected to outweigh this drawback. As advantages can be mentioned:

- the same structure of high-level policy and code of deontology will contribute to the acceptance of security measures by health care professionals;
- the same or a highly similar approach for risk analysis will contribute to acceptance of risk analysis and a rationalized selection of protection measures;
- the same or a highly similar security approach in design and implementation, will not only contribute to easier adaptation of personnel that moves to another organization, but also to a more uniform market for suppliers of health information systems;
- uniformity in application of new techniques, like encryption, will facilitate secure interconnection of information systems from different institutions.

In Europe, the standardization organisation CEN (European Committee for Standardization) recognized the importance of standardization in the field of medical informatics. It installed Technical Committee 251 (TC251) in 1991 to deal with this field under the chairmanship of Dr Georges de Moor from Belgium. Under the umbrella of TC251 are seven working groups. Working group 6 deals with Health Care Security, Privacy, Quality and Safety with Dr Louwerse from The Netherlands as convenor. It is the policy of CEN to cooperate with standardization bodies in other parts of the world. As far as is known, TC251 is the first (and only) standardization committee for security in health informatics. The working group has submitted two proposals to TC251 to install project teams. The success of these attempts to arrive at standardization will depend heavily on the support from both the medical informatics professionals and the health care institutions.

6. Concluding Remarks

In this review several security issues in health information systems have been described. Although most of these issues are also relevant for other application domains, it has become clear that security issues deserve our attention, security should not be an add-on, but an integral part of the design, implementation and operation of health information systems. The health information systems are still evolving, they support a wide range of functions in the health care institutions, also functions that directly relate to patient care. The quality of health care is becoming dependent on the quality of the information supplied. Applied informatics in health care is still rather young; emphasis has been till now on the realization of the systems in a technical and implementation sense; the risks for negative effects on confidentiality, integrity and availability deserve more attention now that the systems have become mature. The interest in security might be triggered by serious incidents; it is our responsibility to react before such incidents occur. IMIA working group 4 tries on the one hand to stimulate cooperation in this field by organizing working conferences, and on the other hand tries to increase awareness and spread ideas by organizing workshops and tutorials during medical informatics conferences. The next working conference *Caring for Health Information* will take place on 13-16 November 1993 at Heemskerk, The Netherlands. Security should not be a hobby of some interested people, it is an essential aspect of each health information system.

References

[1] Griesser GG, Bakker A, Danielsson J, et al. , eds. *Data Protection in Health Information Systems, Considerations and Guidelines.* Amsterdam: North-Holland Publ. Comp., 1980.

[2] Commission of the European Community. *ITSEC: Information Technology Security Evaluation Criteria.* Luxembourg: Office for Official Publications of the European Communities, 1991.

[3] *Council of Europe Regulations for Automated Medical Data Banks.* Recommendations R(81). Strasbourg, 1981.

[4] Westin AF. *Computers, Health Records and Citizen Rights.* Washington DC: National Bureau of Standards, 1976.

[5] Griesser GG, ed. *Realization of Data Protection in Health Information Systems.* Amsterdam: North-Holland Publ Comp, 1977.

[6] Griesser GG, Jardel JP, Kenny DJ, Sauter K, eds. *Data Protection in Health Information Systems, Where do we Stand?* Amsterdam: North-Holland Publ Comp, 1983.

[7] The Commission of the European Communities DG XIII/F AIM. *Data Protection and Confidentiality in Health Informatics.* Amsterdam: IOS Press, 1991.

[8] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data: *SYN 287.* Luxembourg: Office for Official Publications of the European Communities, 1992.

[9] Louwerse CP, Kouwenberg JML. Data protection aspects in an integrated hospital information system. Comput Security 1984; 4: 286-9.

[10] Gritzalis D, Tomaras A, Katsikas S, Keklikoglou J. Data security in medical information systems, the Greek case. Comput Security 1991; 2: 141-19.

[11] ISO7498-2 89 ISO: Information processing systems- Open Systems Interconnection- Basic Reference Model- Part 2: Security Architecture, 1989.

[12] Bakker AR. Data protection and security issues of PACS. In: *Proceedings SPIE Medical Imaging IV.* SPIE Vol 1654, 1992: 509-5.