Medical Informatics Europe '97
C. Pappas et al. (Eds.)
IOS Press, 1997

Some Systems Implications of EU Data Protection Directive

Dr Barry Barber and Dr Francois-Andre Allaert,
Health Data Protection Ltd, Birmingham, UK
Dept de Biostatistiques et Information Medicale, Dijon, France
EU ISHTAR Project partners

The EU Directive "on the protection of individuals with regard to the processing of Personal data and on the free movement of such data" is examined from the point of view of the requirements imposed on the automatic systems processing Personal Health Data and on the relevant implementation timescales.

1 Introduction

At the present time we do not know exactly how the various provisions of the European Union Directive 95/46/EC, "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data" [1] will be interpreted but it can be expected to usher in a New Data Protection regime for most of the European Union. It aims to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" [Art 1.1] and to facilitate "the free flow of Personal Data between Member States" of the European Union [Art 1.2]. In effect the Directive defines "Data Privacy" for the EU for the next few decades. The text is an agreed, compromise, text which provides a variety of options for Member States which they may chose to exercise when framing their national legislation. It extends the scope of the Data Protection arrangements demanded by Council of Europe Convention 108 [2] by requiring, amongst other things, that sound, image and manual data [Art 2(c) "personal data filing systems"] are all brought within the scope of this new legislation. At this stage in the development of new legislation it is far too early to be sure of how the law will be developed and interpreted but, yet, informaticians and systems engineers must begin to address the likely systems implications of the Directive as any necessary facilities must be in place in respect of "new processing" by 24 October 1998 at the latest. The presentation represents a prudent and conservative systems engineer's approach to the likely systems requirements. When the full legal force of the new legislation becomes apparent, it may be that some of the requirements will prove to be unnecessary because the law is not interpreted as stringently as the strict reading of the words might suggest. However, the history of Data Protection is that initial requirements tend to be interpreted in a strengthened fashion as the Data Protection Commissioners and the courts review practice in the light of the specified legal texts. In this context it may be expected that the processing of Special Categories of Data, including Personal Health Data, which is prohibited under Article 8 unless special safeguards are in place, will tend to attract the more stringent safety measures as time goes by. Furthermore, as faster and more capable technology becomes available, practices which would have been prohibitively resource consuming or expensive become standard practice for organisations that do not wish to be negligent. Correspondingly, such technologies reduce the protection provided by previously adequate measures of Data Privacy and, hence, establish the need for further safeguards.

2 Implementation Timescales

Article 32 of the Directive indicates that national legislation is required by 24 October 1998 and that there is an exemption for "processing that is already under way on the date the national provisions....enter into force" which allows three years from that date for such processing to be brought into compliance. In order to test whether any processing of Personal Data is in process, it would appear that one only needs to issue a Subject Access Request. If the result is positive, then "some processing is already under way" otherwise no processing is under way. The simplicity of this test is that it is logical and quite unambiguous. The exemption does not refer to "processing systems" but to "processing" and it does not allow as much time for compliance as appears at first reading of the text. The implication is that all "new processing" will have to comply by 24 October 1998 at the latest and in systems terms this leaves little time for the systems development and testing that may be required. The issues relating to manual files or "Personal Data Filing Systems" are more complex and do not immediately impinge upon the systems required for automated processing, although they may have the effect of speeding the process of computerising some major files.

3 Health Care Requirements

The sensitivity Personal Health Data is recognised in Article 8 of the Directive which is concerned with the processing of special categories of data. The key issues in Health Care arise from the well established need for confidentiality together with the even more serious requirements for the integrity and availability of the patient data required where the information systems are concerned with the active treatment of patients and where patients may suffer damage or death if the information on which their treatment is based is either wrong or missing. Risk analysis using CRAMM [3], has illustrated the Health Care issues arising from situations where information systems are used as an integral part of the treatment process [4,5]. The effect is that where Personal Health Data are simply recorded for research or other purposes but not utilised directly in the processes of delivering Health Care, the key issue is that of confidentiality. Confidentiality has been clearly recognised by Health Care Professionals as vital to patient confidence in the caring processes [6 - 13]. The AIM SEISMED project [Secure Environment for Information Systems in MEDicine] developed this work on a European basis and issued a set of guidelines for routine use in Health Information Systems [14,15]. These guidelines have been developed as a self-consistent set to be used by Managers, Users and Technical staff. They were developed in a fashion consistent with the EU Data Protection Directive and the work of the Council of Europe on the Protection of Medical Data [16]. The Health Telematics ISHTAR project is carrying out further elaboration and validation of these Guidelines at 10 centres [17].

4 Developing Standards for Health Information Systems

It had always been envisaged that computer controlled systems of clinical care would be developed in which the delivery of care was handled autonomously by a computer system but that such "safety-related systems" would require very special design and testing. The beginnings of such safety standards are outlined in the recent standardisation work of the International Electrotechnical Commission [18 - 20] and in the requirements for handling medical devices [21].

However, the advent of Health Information Systems that are at the heart of the processes of delivering care, has led to the potential for causing damage to patients despite the fact that the systems are not directly connected to patients in the sense of acting as a conventional medical device. A clinician is located in the "air gap" between the patient and the information system but where that clinician does not examine the information provided by the system in a critical fashion or where he is unable to obtain information from the system, it is possible for him to provide inappropriate care or fail to provide appropriate care as a result of which the patient may be

damaged or even die. The reasons for such a failure may be various, the clinician may be tired after a long period on duty, he may be worried about family or other matters, he may not have been trained properly but for whatever reason, a cross check is not done that could have revealed the problem. Such problems arise at inquests but until relatively recently they have not involved computerised information systems. As a result of these considerations, the European standards body for Medical Informatics [CEN Technical Committee 251 Working Group 6] has developed a standard [22] that should be out for ballot shortly which seeks to classify Health Information Systems according to their security features in terms of their requirements for confidentiality, integrity and availability and to provide a set of appropriate protection measures for the various categories of system.

5 System Requirements

a) Security

Article 17 of the EU Directive requires "appropriate technical and organisational measures to protect personal data....in particular where the processing involves the transmission of data over a network" which have "regard to the state of the art and the cost of their implementation" and are "appropriate to the risks represented by the processing and the nature of the data to be protected". These requirements need to be in place as soon as the national legislation becomes effective. In addition, the approach taken by the Directive effectively mandates the use of Risk Analysis. Inadequate security will certainly breach the requirements of the Directive and can render the "Controller" liable for negligence under Articles 22 - 24 which are concerned with Judicial Remedies, Liability and Sanctions. The issue of the interpretation of the text in Article 23.2 which allows that:-

"The Controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage"

could be significant as usually the controller will not be directly responsible for a security breach. It is more likely that his negligence may arise from the failure to implement some security measure, and hence left open some system vulnerability, which a reasonable person would have implemented if he was knowledgeable about the current practice and costs in Information Systems Security and if he had understood that likely impact on his patients or his organisation of a security breach. It is likely that prudent hospitals will ensure that they have appropriate security audits commissioned so that they can, at least, prove that they have taken these issues seriously and ensured that all reasonable measures have been installed.

Where Personal Health Data, or other Article 8 Special Category Data are involved, and where these data are networked, higher levels of security will clearly be appropriate. In the networking context, it is difficult to envisage any current alternatives to the use of cryptographic security services. Digital Signatures are likely to be required to ensure that information has not been tampered with and that its origin has been securely authenticated and Personal Health Data are likely to need to be encrypted appropriately when they are sent over open networks. These facilities will be greatly assisted with the widespread availability of a networking infra-structure that provides such services together with Trusted Third Parties and smart cards that can hold the private keys and the associated certificates. Work is in progress on these issues both nationally across Europe and within EU projects the TrustHealth [23].

b) Rectification, Erasure and Blocking

Article 12(b) allows Data Subjects to secure the rectification, erasure or blocking of their

Personal Data where these data do not comply with the requirements of the Directive, "in particular because they are inaccurate or incomplete". Facilities are required to allow this to happen. In general, in Health Care it will be appropriate to block the Personal Data in question so that the clinicians have access to the information but yet it is clearly marked as "inaccurate or incomplete" and is not made available to Third Parties.

c) Third Party Disclosures

Where Personal Data have been rectified, erased or blocked, Data Subjects can require that the Controller notifies Third Parties of this rectification, erasure or blocking "unless this proves impossible or involves a disproportionate effort". This clearly requires a Third Party Disclosure Register of some sort to be built into the systems audit trail and it is difficult to see that this would be an unreasonable requirement bearing in mind that Special Category Personal Data are being passed to Third Parties. It might be that the existing audit trails of some systems would be adequate for this task but it is likely that a special register will be required unless this requirement turns out to be very infrequently required. Furthermore, it might be desirable for the register to be kept as part of the patient record and to include all recipients of Personal Health Data rather than simply Third Parties.

d) User Authentication

In order to enable these matters to be resolved, it is important that all users of the information system should be properly authorised and authenticated. This is a basic security requirement of all information systems but the arrangements in many Health Care settings allow systems to be logged-in all days and utilised by whom so ever requires to use the system or else users freely share their passwords with colleagues. These practices must be prohibited as systems become an integral part of the delivery of Health Care. If no-one knows who is using the system or entering information into the system, then it can only mean that the system is of no particular importance. Such an approach would not be accepted in the context of the written Medical Record. This requirement for authentication of system users is particularly important where Third Parties are given access to Health Information Systems as they are subject to quite different rules in the Directive. This practice is becoming much more common where the delivery of care involves multi-professional teams, shared care between hospitals, community care providers and general practitioners.

e) Data Origin and Consents

The Directive has a number of Articles concerned with the origin of Personal Data [Arts 10 & 11] and the consents for data usage [Arts 7 & 8] and transmission across borders where there is no "adequate level of protection" [Art 26]. It may be that, eventually, it will be necessary for information systems to record the basis for processing and these various consents in a clear and unambiguous fashion and as a fundamental part of the patients' record.

6 Conclusion

The EU Directive establishes a number of requirements for Health Information Systems which need to be considered and addressed now if the next generation of Health Information Systems are to be compliant with its requirements as well as being responsive to Health Care needs in the next century. Digital Signatures are currently thought to be the most appropriate method of secure authentication and verification of the integrity of the information contained in either messages or files. Article 17 is especially concerned with the issues of processing involving

transmission over a network. This appears to mandate the use of encryption for confidentiality where such services are required, for instance in the transmission of Personal Health Data over open networks, and the use of Digital Signatures for the authentication of the integrity and origin of messages. These facilities will need to be built into the architecture of Health Information Systems over the coming years but the Third Party Disclosure Register remain a major requirement to be built into EU systems within the next few years.

References

1 European Union Directive 95/46/EC, "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data", OJ L281/31 - 50, 24 October 1995

2 Convention "For the Protection of Individualise with regard to Automatic Processing of Personal Data", Council of Europe Convention 108, January 1981, ISBN (1982) 92-871-0022-5

3 "CRAMM User Guide", issue 1.0, April 1996, CRAMM software version 3.0, The CRAMM Manager, PO Box 1028, London N1 1UX

4 "Worst Case Scenarios: the Legal Consequences", Barber B, Vincent R and Scholes M, pp 282 - 288, "Current Perspectives in Healthcare Computing 1992", ed Richards B et al, pub for British Computer Society by BJHC Weybridge, ISBN 0 948198 12 5

5 "The Use of the CCTA Risk Analysis and Management Methodology [CRAMM] in Health Information System's", Barber B and Davey J, pp 1589 - 1593, in "MEDINFO 92", ed Lun KC et al, pub for IMIA by North Holland, Amsterdam, 1992, ISBN 0 444 89668 6

6 "Data Protection in Health Information Systems: Considerations and Guidelines", Griesser, G et al, pub for IMIA WG4 by North Holland, Amsterdam, 1980, ISBN 0 444 86052 5

7 "Data Protection and Confidentiality in Health Informatics: Handling Health Data in Europe in the Future", ed EU Commission, DG XIII/F AIM, vol 1 in Studies in Health Technology and Informatics, IOS Press, Amsterdam, 1991, ISBN 90 5199 052 9

8 "Data Protection in Health Information Systems: Where Do We Stand?", Griesser, G et al, pub for IMIA WG4 by North Holland, Amsterdam, 1983, ISBN 0 444 86713 9

9 "Caring for Health Information: Safety, Security and Secrecy", ed Barber et al, pub for IMIA WG4 Elsevier, Amsterdam, ISSN 0020-7101 [also in Int J Bio-Medical Computing, vol 35, Supplement February 1994

10 "The Six Safety First Principles of Health Information Systems: A Programme of Implementation" in ref 7 pp 297-314

11 "The Security of the Electronic Health Care Record - Professional and Ethical Implications", Gaunt N and Roger-France F, pp 10-22 in ref 14

12 "Security of Health Information Systems in France: What we do will no longer be different from what we tell", Allaert FA and Dusserre L, pp 201- 204, in ref 9

13 "Transborder Flows of Personal Data in Europe: Legal and Ethical Approach", Allaert FA and Dusserre L, pp 1572 -1575, in "MEDINFO 92", ed Lun KC et al, pub for IMIA by North Holland, Amsterdam, 1992, ISBN 0 444 89668 6

14 "Towards Security in Medical Telematics", ed Barber B et al, vol 27 in Studies in Health Technology and Informatics, IOS Press, Amsterdam, ISBN 90 5199 246 7

15 "Data Security for Health Care" ed the SEISMED Consortium, volumes in Studies in Health Technology and Informatics, IOS Press, Amsterdam, 1996
Vol I Management Guidelines ISBN 90 5199 264 5 (series vol 31)
Vol II Technical Guidelines, ISBN 90 5199 265 3 ((series vol 32)
Vol III User Guidelines, ISBN 90 5199 266 1 ((series vol 33)

16 The Protection of Medical Data, draft Recommendation for the Council of Europe, June 1996

17 ISHTAR project, Implementing Secure Healthcare Telematics Applications in Europe, EU Fourth Framework, HT1028, 1996 - 1999

18 Draft International Standard IEC 1508 Functional Safety Related Systems Parts 1 - 7, June 1995

19 "Safety and Security of Information Systems", Shaw R pp 190 - 199 in ref 14

20 "Standards in Medical Software", Bennett PA, pp 197 - 213 in ref 9

21 EU Council Directive "Concerning Medical Devices", OJ L169/1 - 43, 14 June 1993 Directive

22 Security Categorisation and Protection for Healthcare Information Systems, draft CEN prENV, ref CEN TC251/WG6 N96-060, 1996-10-26

23 TrustHealth project, EU Fourth Framework Trustworthy Health Telematics 1, HT 1051, 1996 - 1997

Medical Informatics Europe '97
C. Pappas et al. (Eds.)
IOS Press, 1997

Patient Care Evaluation Studies: Applying this concept of quality management in oncology

S. Hölzer, J. Dudeck, *Institute of Medical Informatics*
Justus-Liebig-University Gießen, Heinrich-Buff-Ring 44, D-35392 Gießen, Germany

Abstract: Patient Care Evaluation Studies are valid tools of quality management in oncology. With the use of modern methods of medical informatics, epidemiology and biometrics, the acceptance of tumor documentation in the clinical routine will be improved. We will describe the ideas behind the concept of the PCE studies.

1. Introduction

The primary goals of the Patient Care Evaluation Studies (PCES) are to monitor changing patterns of care and survival trends in oncology. This concept has been developed by the Commission on Cancer (COC) of the American College of Surgeons (ACS) and established since several years in the United States. As the results of these studies reflect the standards and time trends of diagnostic, therapy and follow-up in the management of cancer patients they have become valid tools of quality assurance in oncology (1,2).

2. Idea and study content

In a first step, we decided, in cooperation with the Commission on Cancer, to start a Patient Care Evaluation Study in 1996 as a pilot project in Germany. The intention is the integration of this tool in the quality management process of oncology in the Federal Republic of Germany and to compare the data in the two involved countries. We decided to join the PCES of thyroid cancer which is one of the chosen tumor entities for the year 1996. Different reasons and reflections, mostly the clinical aspects of these tumors, have led to this choice.

3. Clinical aspects

Carcinoma of the thyroid gland is an uncommon cancer but, nonetheless, the most common malignancy of the endocrine system. Differentiated tumors (papillary or follicular) are highly treatable and usually curable. Poorly differentiated cancers (medullary or anaplastic) are much less common, are aggressive, metastasize early, and have a much poorer prognosis. The treatment includes, depending on the stage and histological type, surgical, radio-therapeutical, hormonal and chemotherapeutical approaches. The treatment in Germany is in parts different compared to the USA. There are only a few known important prognostic factors, such as age, whereas the prognostic significance of lymph node status is controversial. Prospective randomized clinical studies are rare. New diagnostic technologies in the follow-up of patients such as PET are not sufficiently evaluated and its sensible and economic use is unknown. Physicians for nuclear medicine mostly practice a part of the treatment and diagnostic procedures as well as the follow-up (3-9).

4. Epidemiological aspects

Based on the database of a regional German epidemiological tumor registry we have estimated the occurrence of about 2500 to 3000 cases of primary diagnosed patients with thyroid neoplasms per year. The incidence rates in Germany are actually 6,0 for females and 1,6 for males in a population of 100.000. The incidence of this malignancy increased over the past decade (10).

5. Data form

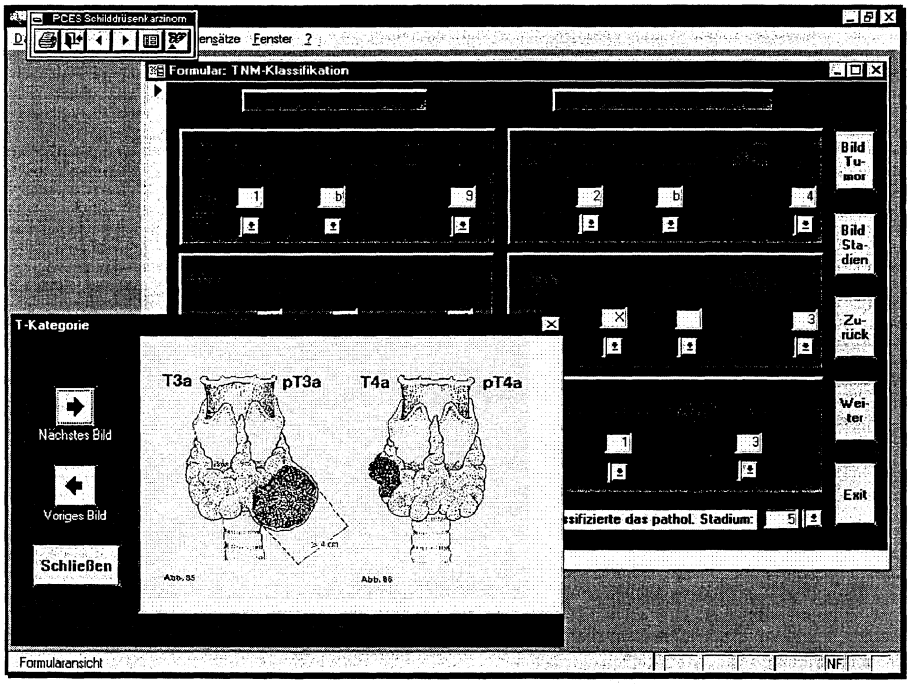
In a second and most important step, we evaluated the American data forms of the PCES of thyroid cancer and adapted it to the circumstances of the German medical infrastructure. In collaboration with surgeons, endocrinologists, physicians for nuclear medicine, radiooncology, pathology and their corresponding medical organizations, we created a new data form, implementing all revised items of the American PCES. Each specialist contributed his ideas and demands in order to get the best view of standards concerning diagnostic, therapy and follow-up. As the result of this work, the prospective PCES includes, for example, detailed information about the execution and side effects of surgical treatments, radio-iodine and hormonal therapy as well as the histological criterion and extend of disease. In contrast of the study of the COC, we want to document the complete follow-up for the included patients over the next five to ten years. The questions that should be responded by this study are shown in the following table:

Questions and goals of the PCES of thyroid cancer:

- What are the current age and sex ratios of patients with thyroid cancer?
- How is the tissue diagnosis established?
- Which methods of diagnosis are used most frequently?
- Are there any predisposing factors and do they have prognostic impact?
- What are the presenting symptoms of thyroid cancer?
- Is the disease being appropriately evaluated?
- What is the role and contribution of imaging studies and biopsy in diagnosis?
- What is the distribution of the stage of the disease?
- What techniques are used for operation?
- What is the impact of surgical therapy on complications and disease control?
- What are the operative morbidity and mortality rates?
- What is the impact of radio-iodine therapy, radiation and hormonal therapy on complications and disease control?
- Which are the differences in the patient care between the Federal Republic of Germany and the United States?
- Are supposed prognostic factors indeed predictive of outcome?

6. Data Base Management System

On account of the absence of Comprehensive Cancer Centers and of disseminated computerized cancer data management tools that are established in the American healthcare system, we have built a data base application allowing the input of the required items and data export to the study head office for further central statistical analysis and interpretation. We made this thyroid cancer data base program available for both stand alone and network version. Its size and graphical user interface allow the use in the medical routine with the personal computer on the physicians desktop as well as on tumor registries. An example of a data form is shown in the following figure:



Form of the thyroid cancer database management system

7. Distribution of results

The results and statistical analysis of the German PCES and the comparison with the data of the American pendant will be available to all involved hospitals, clinical departments and medical organizations. The interpretation will be performed by each medical discipline for single topics in accordance with their specific interests. The essentials, conclusions and recommendations will be presented on-line via world wide web (11). This allows a fast way to set and change recommendations and to give a current overview of standard in the clinical management of neoplasms. In addition, we will develop a database application for an internet information server to allow the dynamic platform independent access to a selected part of statistic analysis for further processing (12,13).

8. Discussion and conclusion

PCE studies play an important role in oncology because the concept intervenes with different mechanisms of the process of quality assurance. PCE studies contain the documentation of patient care at multiple levels of diagnostic, therapy and follow-up as a part of the process quality (14-17). The structured and long term documentation of the time of survival in dependence on therapeutical modalities is essential for the outcome quality. The responsible institution has to play an active role including identification of issues, study design, data check and interpretation of results. In interdisciplinary cooperation the development of action plans should be performed. The acceptance of documentation in the clinical routine has to be improved in order to assure effective and economic long term quality management in medicine (14,15). Improvements can be achieved by the use of all available methods of medical informatics, statistics and biometrics.
Prospective clinical studies of the less common thyroid neoplasms are difficult to conduct and require a high degree of multicenter cooperation. They require a long period of follow-up and the cooperation of a multitude of clinical departments of different medical disciplines, before meaningful results are generated. As a consequence, existing multicenter groups tend to avoid initiating such trials. With a well thought-out and long term planned tumor documentation the current issues of the state of the art of patient care could be characterized and different diagnostical and therapeutical options evaluated against each another. On this basis various types of specific clinical trial could be initiated with more precise questions and a smaller number of required patients. An interdisciplinary and multidisciplinary approach should include the cooperation of clinical physicians, physicians of medical informatics and medical registrars. The infrastructure and arrangement between the involved medical disciplines have to be realized by an adequate responsible institution. In this case the Institute of Medical Informatics at the University of Gießen acts as a mediator, responsible for the coordination and implementation of different suggestions, the data base management, checking the quality of incoming data, statistical analysis, distribution of results and interpretations. In this stage of the current project, we want to evaluate the feasibility of such studies under the technical and personnel conditions of the German healthcare system.

9. Perspective

In the near future we plan to apply the described concept to various types of tumor entities like breast, prostate cancer and melanoma parallel to the studies in the USA and we want to involve other European countries. We make the effort to improve the process of quality management using all available methods of medical informatics, statistics and biometrics. The PCE studies promote the interdisciplinary cooperation both on national and international level. Their role and sensible use will be demonstrated.

References

1. Steele GD, Jr., Jessup JM, Winchester DP. Annual Review of Patient Care. National Cancer Data Base 1995.

2. Clive RE. A National Quality Improvement Effort: Cancer Registry Data. Journal of Surgical Oncology 1995;58:155-161.

3. Reiners C. Imaging methods for medullary thyroid cancer. Recent Results Cancer Res 1992;125:125-145.

4. Reinhardt M, Guttenberger R, Slanina J, Frommhold H, Moser E. [Indications for percutaneous radiotherapy in carcinoma of the thyroid gland. Freiburg consensus]. Radiologe 1995;35:535-539.

5. Reinhardt MJ, Moser E. An update on diagnostic methods in the investigation of diseases of the thyroid. Eur J Nucl Med 1996;23:587-594.

6. Mazzaferri EL, Jhiang SM. Differentiated thyroid cancer long-term impact of initial therapy. Trans Am Clin Climatol Assoc 1994;106:151-168.

7. Mazzaferri EL, Jhiang SM. Long-term impact of initial surgical and medical therapy on papillary and follicular thyroid cancer [see comments] [published erratum appears in Am J Med 1995 Feb;98(2):215]. Am J Med 1994;97:418-428.

8. Sellers M, Beenken S, Blankenship A, Soong SJ, Turbat Herrera E, Urist M, Maddox W. Prognostic significance of cervical lymph node metastases in differentiated thyroid cancer. Am J Surg 1992;164:578-581.

9. DeVita. The Thyroid Gland. Cancer: Principles and Practice of Oncology 1989;3rd:1269-1284.

10. Saarland. Morbidität und Mortalität an Bösartigen Neubildungen. Krebsregister Saarland 1995;Jahresbericht 1992.

11. Adelhard K, Hölzel D, Klammert A, Schmidt M. Interactive Access to Clinical and Epidemiological Cancer Data. Medical Informatics Europe 1996;113-117.

12. Cimino JJ, Socratous SA, Clayton PD. Internet as clinical information system: application development using the World Wide Web [see comments]. J Am Med Inform Assoc 1995;2:273-284.

13. Lindberg DA. Global information infrastructure. Int J Biomed Comput 1994;34:13-19.

14. Wagner G, Hermanek P. Organspezifische Tumordokumentation. Springer 1995.

15. Dudeck J, Wagner G, Hermanek P. Basisdokumentation für Tumorkranke. 4th Ed. Springer Verlag, 1994.

16. Hutter RVP. Quality assurance in cancer care. Pathol Cancer 1989;64:244-248.

17. Selbmann HK. Thesen zur Qualitätssicherung in der Krankenversorgung. Bayr Ärztebl 1992;47:338-342.

Medical Informatics Europe '97
C. Pappas et al. (Eds.)
IOS Press, 1997

Forming a Health Care Incident Reporting Scheme

Konstantinos G. Mavroudakis[1] , Sokratis K. Katsikas[1] and Dimitris A. Gritzalis[1,2]
[1] *University of the Aegean, Dept. of Mathematics, Karlovassi 83200, Greece*
[2] *Athens University of Economics & Business, Dept. of Informatics, 76 Patission St., Athens 10434, Greece*

Abstract. In this paper the initial design steps of an Incident Reporting Scheme for Health Care are presented. The results of a short survey for the determination of Health Care user needs and expectations from such a scheme are given. The paper outlines a concise description of the proposed system and presents the conceptual model of the IRS database, and the developed prototype version of this database. Finally, future steps and security issues are described.

1. Introduction

Information has become the most precious asset in all types of organisations. Hence, it is imperative that information and the associated information services need to be protected to ensure a high level of information confidentiality, integrity and availability at all times. The use of Information Technology (IT) within Health Care Establishments (HCEs) increases very fast. Information Systems are increasingly being developed and used in a widening area of applications. HCE staff tends to depend all the more on computerised Health Information Systems (HISs) in order to perform their everyday functions. Moreover, HISs no longer process only hospital and financial data, as they once did. In addition, HCE staff use HISs to assist themselves in diagnosing, record information of a purely medical nature or even to assist themselves in patient treatment, i.e. modern HISs process medical data as well. These data are related directly to identifiable persons, their illness, their treatment, and sometimes their habits, hence they are extremely sensitive. It is obvious that confidentiality, integrity and availability in the treatment of Health related data is needed.

Another fundamental change in the Health Care community is the transition from the traditional model of a stand-alone HIS, that is the HIS operating within the boundaries of a single HCE, to the inter-networked HIS, that is a HCE's HIS interconnected to HISs of other HCEs or even third parties, over national or international Wide Area Networks (WANs) with the capability of transmitting data, voice and images. This increased dependency of HCEs upon HISs, brings forth the paramount need of preserving data security in the processing of data by computerised HISs [1].

The increasing use of and dependence on interconnected Local Area Networks (LANs) and WANs while bringing important new capabilities, also brings new vulnerabilities and increases the possibility of a security breach or incident to occur [2]. Computer security

breaches could cause organisations or agencies to face extreme expense in productivity, significant damage to their systems, loss of funds, and damage to their reputations [3-4].

In response to the Internet worm incident of November 1988, the Defence Advanced Research Projects Agency (DARPA), the National Institute of Standards and Technology (NIST), the National Computer Security Centre (NCSC), and a number of other agencies and organisations decided to take actions to enhance Internet security [5]. A recommendation from the NCSC post-mortem workshop [6] was that a formal crisis centre be established to deal with future incidents and to provide a formal point of contact for individuals wishing to report problems. As a result, the first Computer Emergency Response Team (CERT) was established by DARPA. One of the primary activities of a CERT (alternatively Incident Response Team - IRT) is to respond to computer security incidents with a corrective or responsive action [7].

Since that time a large number of CERTs and other similar initiatives have appeared [8-11]. It was clear that management should focus on the nature of threats, their possibility of occurrence which depends on system vulnerabilities, and their potential impacts. This indicated a need for information about the nature and frequency of past threat occurrences (incidents). In turn, systems for reporting and recording of security incidents were necessary, in order to ensure both these needs. These systems are known as Incident Reporting Schemes (IRS).

An IRS provides information that results from the processing of incident data sent from different member organisations or from other IRSs, and is prepared by IRS operators in the form of regular reports or alerts on issues which may need immediate investigation. The information which these reports present will reflect large number of actual experiences from different organisations. This assists member organisations to better understand what they need to protect and why they need to protect it. In turn this should produce an improved understanding on how appropriate protection should be planned and implemented.

The use of interconnected HISs in Health Care, the high sensitivity of health related information, the characteristics that differentiate them from other environments[12], and the demand for the provision of practical measures neccessitate the development of a Health Care Incident Reporting Scheme (HIRS). Such a task has been undertaken within the EU Health Care Telematics Programme, Project HC1028 ISHTAR (Implementing Secure Healthcare Telematics Applications in EuRope).

2. Requirements for a HIRS

The first step towards designing and implementing a HIRS was to conduct a short survey among HCEs, in order to record their needs and expectations from such a scheme. A questionnaire was prepared and sent to the ISHTAR Verification Centres (VCs), i.e. a group of ten European hospitals. The VCs involved in the survey employ in total approximately 17500 employees, with individual sizes varying between 1500 and 5000 people. The results of the survey are summarised in the following table (Table 1).

In the mean time, a prototype version that demonstrates some of the functions of the HIRS was developed, based on the information collected from existing HIRSs. This pilot system is being gradually expanded and refined to meet the user expectations for the HIRS database.

Requirement	User views
Audience boundary	European
Hardware to be used	PCs or Network
Threats	Exhaustive covering
Impacts	Exhaustive covering
Components affected	Data & Services
Metrics of impacts	Exhaustive covering
Notifier of incidents	Security or Data protection Officers
Obligation of notification	Voluntary
Means of notification	Standard form
Media for notification	e-mail or post letter
Reporting	Exhaustive covering
Security	HIRS database
	Communications
	Management
Validation for Notification	HCE security officer with HIRS operator
Reporting frequency	Immediate or periodic
Dissemination mode	• Health Care profession press • Electronic reports (e.g.,WWW) • Restricted recipients

Table 1

3. Definition, functions and architecture of the HIRS

In this section, a reference model is presented in order to structure the Incident Reporting Scheme (IRS). Its aim is to allow organisations in Health Care to interact with the proposed IRS, in order to be provided with facilities such as comparing results, improving information quality and a more accurate view of the threats and vulnerabilities that member organisations are susceptible to. The main building blocks suggested in this model are incidents, threats, vulnerabilities, impacts, assets, impact metrics, user organisations, reports, and the IRS operator. All the above concepts are further subdivided to different types in the model. An appropriate entity relationship model has been designed to include the above concepts and their relationships. This model has been applied in the development of the HIRS database management system.

3.1 Incident Reporting Process

The HIRS architecture suggests three main tasks: incident collection / notification, incident data processing by the HIRS and generation of reports (Fig. 1).

3.1.1 Incident notification

The person with the responsibility to notify incidents i.e. the HCE notifier uses a number of telephone calls, faxes, e-mails or other media to notify the incident to the HIRS. An appropriate validation and authentication procedure is applied by the HIRS operator to verify that the notified event is a genuine incident and that this event originates from this HCE.

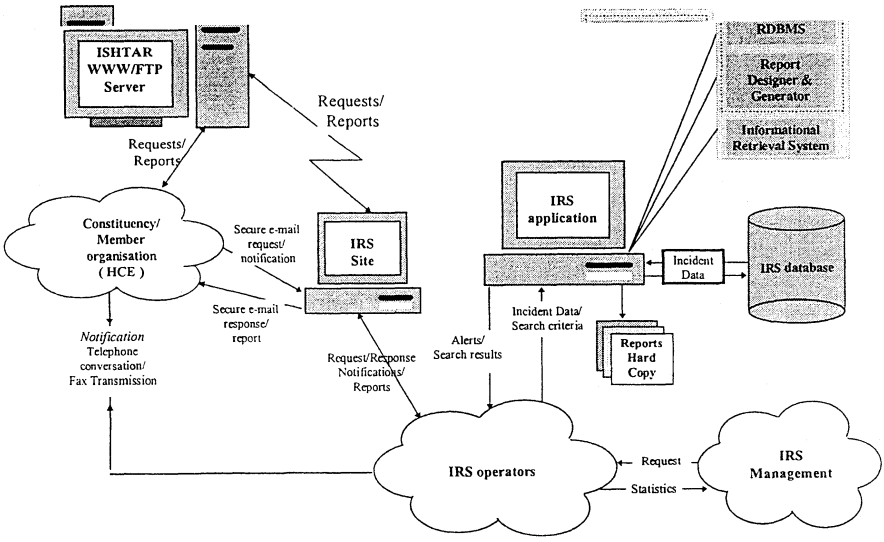


Figure 1

3.1.2 Incident data processing

The HIRS will process the collected incidents and the result of this task should proc useful and meaningful reports, enhanced with information that may stem from sir incidents that already have been registered at the HIRS database. The reference model serve data anonymity by hiding any relative information once it is obtained by the H operator. Mechanisms for achieving that will focus on the encryption of names and c concerning the HCE involved, departments and people employed. It should be noticed the HIRS operator must comply with any term imposed in a contractual agreement betw the client-HCE and the provider-HIRS concerning the security issues. Such binc procedures will act as a deterrent to any arbitrary action taken by the HIRS operato addition, confidentiality will be kept at the maximum degree by physically isolating HIRS database containing the actual incident data.

3.1.3 Reporting

The HIRS will support HCEs providing them with several different report types. Tl include alerts, statistics, regular reports, and special or ad hoc extraction reports. The H reporting facility should take into consideration odd incidents that may occur in diffe organisations but show signs of similar behaviour.

A number of reports based on anonymous incident data will be available from a V site or from an anonymous FTP site serving remote access by HCEs or the public witl time limitations.

It is proposed that the particular reference model will respond to the inci notifications periodically, for example, on a monthly or on a quarterly basis, althoug cases where immediate action is required the HIRS will produce reports on time.

3.2 The database application prototype

The pilot version for the proposed HIRS presently covers the management of database and the publishing of reports.

Management encompasses the registration of new records along with update deletions where this would be necessary. The HIRS operator will be able to se

appropriate incidents based on a variety of criteria that more or less reflect the way data are structured inside the database. For example, the HIRS operator may select incidents based on a specific type of threat. After selecting the appropriate incidents, the operator will be able to issue a regular report or any other report based on these incidents.

Hardware and software requirements for the development and use of the pilot HIRS database application are Windows 95 operating system, Microsoft Access 7.0, a Pentium PC with 24 MB RAM, 500 MB hard disk space (for 133000 incidents), and a 15'' SVGA Monitor.

4. Conclusions

HCEs are organisations whereby extremely sensitive pieces of information are processed, and consequently, the need for data security is paramount. Security policies require the reporting of security breaches by users to the security officer of the organisation. An HCE will be able to learn from reported information and avoid potentially serious consequences. The increased dependency of HCEs upon HISs and international networks (e.g. Internet), and the previous experience regarding security in interconnected information systems, demand the establishment of a central European HIRS that will collect security breach information from different HCEs. This HIRS will provide useful reports containing this aggregated Health Care experience on security breaches.

A short survey has been conducted among a number of HCEs in Europe, in the context of the ISHTAR project, in order to determine the user needs and expectations from such a HIRS. In the mean time, a prototype for the application that manages the incident data of HIRS was developed to assist on the proper evaluation of the requirements. The scheme is under development. The next step is to provide the framework for security incident handling by the HIRS.

References

[1]. Katsikas S.K., *The SEISMED High Level Security Policy for Health Care*, in Towards Security in Medical Informatics, Barber, B. et al., eds., IOS Press, 1996.

[2]. Pethia R.D., van Wyk, K.L. *Computer Emergency Response - An International Problem,* 1990, ftp://cert.sei.cmu.edu.

[3]. Audit Commission, *Opportunity Makes a Thief: An Analysis of Computer Abuse*, National Report, London, HMSO, 1994.

[4]. Audit Commission, *Survey of Computer Fraud & Abuse*, The Audit Commission for Local Authorities and the NHS in England and Wales, 1990.

[5]. Montz L.B., *U.S. General Accounting Office Report Highlights the Need for Improved Internet Management*, in Denning P.J. (ed.), Computers Under Attack: Intruders, Worms, and Viruses, ACM Press, 1990.

[6]. Spafford E.H., *Crisis and Aftermath*, in Denning P.J. (ed.), Computers Under Attack: Intruders, Worms, and Viruses, ACM Press, 1990.

[7]. TERENA Task Force, *CERTs in Europe*, Final report, October 1995.

[8]. Kossakowski K.P., "The DFN-CERT Experience - Building up a new CERT within Europe", in *Proc. of INET'94/JENC5,* Internet Society, 1994.

[9]. Schultz E.E., Brown D.S., Longstaff T.A., *Responding to Computer Security Incidents: Guidelines for Incident Handling*, National Technical Information Service (NTIS), July 23, 1990

[10]. Smith D., *Forming an Incident Response Team*, Australian Computer Emergency Response Team, Australia, 1994.

[11]. Wack J.P., *Establishing a Computer Incident Response Capability (CSIRC)*, NIST Special Publication, November 1991.

[12]. Roger France F.H., Gaunt P.N., *The Need for Security - A Clinical View*, in Proc. of IMIA Conference on Caring for Health Information Safety, Security and Secrecy, B. Barber, et al. (Eds.), The Netherlands, November 1993.