LEGISLATIVE ISSUES IN THE PROCESSING OF SENSITIVE PERSONAL DATA IN THE ELECTRONIC PATIENT RECORD

Malliarou Maria [1], Sarafis Paul [2]

1.Captain Psychiatric RN, MSc, PhD(c), 492 General Military Hospital of Alexandroupolis.
2.Lieutenant RN, Hel. Navy, Athens Naval & Veterans Hospital, MSc Health services management H.O.U, MSc Public Health N.S.P.H- Hygienist, PhD-scholar of the Onassis Foundation, Specialty in Infections & Tropical Diseases.

Abstract

Introduction: EPR is an evolving idea determined as a long-term collection of health care information of patients and populations. EPR has gained a great value in the healthcare environment. Its contribution to the improvement of the quality of health care provision, to the reduction of health services' costs, and to the increase of productivity and efficiency of health care professionals, justify its importance.
Purpose / Objective: The purpose of this study was to explore the general legislative status in Greece, E.U., and USA for the protection of sensitive personal data in the Electronic Patient Record (EPR).
Methodology: In preparation for reviewing the literature on the general legislative status in Greece, E.U., and USA for the protection of sensitive personal data in the EPR, a MEDLINE and a GOOGLE search was conducted. Bibliographic review was made with key words "Electronic patient record, sensitive personal data, legislation, security".
Results: Each country in E.U but in America also tries to protect the people's right for a safe handling of personal data included in an EPR by setting the minimum necessary requirements for each health organization that uses it and by creating laws for the same purpose. Greece, following the instructions by E.U, has already legislated in order to protect the EPR's sensitive personal data.
Conclusion: The determination of ethic and legal guidelines and criteria relevant to the electronic collection, processing, and communication of personal sensitive health data, is vital. A potential disclosure of patient's personal data puts in risk the relationship between the patient and the physician or nurse but also the one among the members of the entire society since the patient may be afraid or reluctant to trust to reveal critical information that concern not only his personal health but also the public health.

Keywords: Electronic patient record, sensitive personal data, legislation, security.

Corresponding author:
Malliarou Maria
104, Vizvizi, Alexandroupolis
Greece 68100
Tel:+30 25510 38732
Mob: 6944796499
Email: mmalliarou@gmail.com

Introduction

The electronic patient record is the collection of all health information and is created for every patient who receives treatment, care, or services at each institution or health network, and is maintained for the primary purpose of providing patient care. In addition, it is used for financial and other administrative processes, outcome measurement, research, education, patient self-management, disease prevention, and public health activities. The record contains sufficient information to identify the patient, support the diagnosis, justify the treatment, document the course and results of treatments, and facilitate the continuity of each patient's care.[1] EPRs can offer several advantages and some of them are better legibility,[2]simultaneous access for several physicians at different locations[3]. EPRs can optimize the accuracy, completeness, costs and effects of clinical processes and of their results[4].Therefore, EPRs can provide patient-centered health care. The increasing use of EPRs has brought to the fore concerns about information security and more specifically about the confidentiality of computerized health care data because the diversity of origin and use of health care data create such problems.

The contribution of the electronic patient record towards a qualitative health care, of the reduction of costs of health services, of the increase of efficiency of the professionals of health but also the rests of users of electronic patient health record leads to the recognition of its value and its application and its use in health environment. The better management of information does not only have economically and functional profits, but it improves the quality level of life, as the right information in health matters has decisive impact on the patient care. The automation of all processes that contribute to the benefit of health services, to research and to the reception of critical decisions for the patient's life, makes imperative the need of safety of the systems of electronic patient records in order to ensure the validity, the reliability, the availability of medical information but also the patient's right for secrecy of his personal sensitive data that are concluded in those systems. The application and the operation of safe systems of electronic patient records as long with the suitable measures, the use of safety policies, the application of models, the observation of requirements of laws that are imposed by the international but also by the European community are those that will change the culture of the professional users and those that will lead to a secure management of medical data and of personal sensitive patient data and also those they will diagnose in time the problems that will result from no observation of the above.[5]

The objective of each effort for defense of patient's right of medical and nursing secrecy is to strengthen the confidence of citizens towards the new possibilities of information technologies and also the need for professionals' use of safety measures. The value of health information that is in the patient's record goes far beyond the treatment of patients: the medical research, the public health, the planning of services show the profits from their safe use. The electronic patient record is an evolving idea determined as a long-term collection of medical information for patients and populations. It is evident that the patient's right for confidentiality of his personal data cannot be degraded because of the use of electronic patient record. The application of security policy into the hospital information systems is demanded under law because it must fulfill the demands of safety of the personal sensitive health data as the law 2472 of 1997 compels. So with the combined use of cryptographic tools (algorithms), suitable software, hardware, infrastructures and procedures, it is possible that solutions are offered in order to satisfy the requirements of laws for safety. The Greek legal frame for the electronic patient record is regulated by the legislation that ensures the confidence of communications and the networks as well as the safety of personal data of patient.[5]

Since the creation of the Hippocratic Oath about 400 B.C., protecting the privacy of patients has been an important part of physicians' code of conduct. The worries about confidentiality were exemplified in a

pp:139-148
ISSN:1108-7366, E-ISSN:1791-809X

legal setting by the Hesse Data Protection Act 1970 and the Swedish Data Act 1973 and the US Privacy Act 1974 which covered federal agencies and set out requirements but without a central data protection authority. In the UK, the Younger[6] and Lindop[7] committees considered the issues of privacy in general and data protection in particular and a white paper[8] was developed as a basis for legislation that did not emerge at that time.

The disclosure of patients' sensitive information about mental health, sexually transmitted diseases, adolescent care[9], drug addiction and genetic fingerprints creates many ethical problems.[10] Most professional ethical bodies in Europe give the responsibility for protection of patient records to the health care practitioners. For example, in the UK, the General Medical Council states:

Data protection law in most European countries requires that data be held only for a defined purpose, and for no longer than is necessary[11]. Health data can be used for purposes of administration, audit and performance review but patient identifiers should preferably be removed beforehand so that individual's identity is not revealed by unusual combinations of apparently anonymous data.

Material-Method

Each country in E.U and in USA also tries to protect the people's right for a safe handling of personal data included in an EPR by setting the minimum necessary requirements for each health organization that uses it and by creating laws for the same purpose. Greece, following the E.U instructions, has already legislated in order to protect the EPRs' sensitive personal data. In preparation for reviewing the literature on the general legislative status in Greece, E.U., and USA for the protection of sensitive personal data in the EPR, a MEDLINE and a GOOGLE search was conducted.

FINDINGS

International legal instruments

- **Council of Europe Convention 108**

In 1976 the Council of Europe started working on the preparation of a convention on privacy in respect of data processing while the Organisation for Economic Co-operation and Development started at about the same time considering similar issues from the economic, technical and legal point of view rather than from the human rights standpoint. The Council of Europe's work started from Article 8 of its Convention on Human Rights[12]. The development of Convention 108 became a reality. This Convention 'for the protection of individuals with regard to automatic processing of personal data[13], established the council's view of the appropriate safeguards in respect of the processing of personal data. It drew on the experience of existing national legislation and legislative thinking which has been signed by 22 countries. In a very real sense Convention 108 has set a standard for data protection issues.

- **Council of Europe Recommendation R (81)1**

Recommendation R(81)1 On Automated Medical Data Banks[14], did have some special features that required that medical data banks should have a set of regulations governing its operations and the recommendation specified a minimum set of contents for these regulations. It established the concept of selective access to the identification, administrative, medical and social parts of the medical record and it addressed issues of record linkage. It established the exceptions to subject access as being 'data banks which are used only for statistics or scientific research purposes'. It, also, allowed erroneous data to be kept after it had been corrected 'so far as knowledge of the error may be relevant to further medical treatment or useful for research purposes'. The only aspect of the recommendation that proved unworkable as computing facilities became much more widely available was the requirement to give advance public notice of the establishment of a medical data bank.

- **Council of Europe Recommendation R (97)5**

The Council of Europe's work in the area of biomedicine and bioethics led to the belief that there might be some problems between the requirements of genetic counselling and

pp:139-148
ISSN:1108-7366, E-ISSN:1791-809X

data protection and they revised the Recommendation on Automated Medical Data Banks. There has been an attempt to summarise the desirable situation for health care in Europe and ensure that staff met these standards in their handling of medical data. Their purpose was to ensure patients that their medical data were uniformly protected. Recommendation R (97)5 on the protection of medical data[15] now formally replaces the earlier recommendation and it is likely to become the basis for handling personal health information, including personal genetic information, for a generation. This work was adopted on 12 February 1997. The recommendation concerns all processing of personal medical data except where national law provides other appropriate safeguards in a specific area outside the health-care sector. The status of the Council of Europe's conventions is that of an international treaty, although it is not clear what sanctions might be brought against recalcitrant states. Certainly, this recommendation recommends governments to ensure that its principles 'are reflected in their law and practice' and to ensure wide circulation of its principles 'among persons professionally involved in the collection and processing of medical data'. In addition the recommendation deals with the security of personal medical data, its long term retention, trans-border data flows and the use of data for scientific research. It also addresses issues relating to the personal data of unborn children, legally incapacitated persons, unexpected findings in genetic analyses and various permitted exemptions from specific requirements. The recommendation sets out categories of protective control where measures are required as access to installations, handling of data media, access to system memory, utilisation of systems, separation of categories of medical data, access to networking facilities, data entry, transport of data media and back up arrangements. The general approach is similar to the approach in other documents but it is much more detailed in its requirements.

- **European Community directive 95/46/EC**

The European Community 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'[16] was adopted somewhat earlier than Recommendation R(97)5, on 24 October 1995. Its status is rather different from the convention and the recommendations of the Council of Europe in that the directive is mandatory for all countries within the European Union but its scope is restricted to the legal competence of the European Union law. Member states were required to install legislation implementing the directive by 24 October 1998 but the transition arrangements in Article 32 allowed the full rigor of the national legislation required by the directive to be implemented in stages. The manual 'personal data filing systems' are allowed until 24 October 2007 to comply fully but the data subject's rights of access, rectification, erasure and blocking appear to start not later than 24 October 2001, assuming that such data are likely to be 'processing already under way'. [17, 18, 19]

The directive is based on Convention 108 but it goes beyond the requirements of the convention in a number of respects. The convention makes provision for signatory states to extend its scope by applying its requirements to manual information systems or to legal persons but the directive includes manual systems directly by the definition of 'personal data filing systems'—although with a longer transition period. The security requirements in Article 17 are similar to those required by the recommendation except that the cost of implementing security measures is explicitly included in the process of assessing the appropriate security measures. It allows for the 'blocking' of personal data 'which does not comply with the provisions of this directive, in particular because of the incomplete or inaccurate nature of the data'. This provision is a general extension of that established in Recommendation R (81)1 in the second paragraph of section 6.2. Perhaps the most extensive change is the requirement in Article 12(c) that 'third parties to whom data have been disclosed should be notified of any rectification, erasure or blocking of data' carried out as outlined above 'unless this

proves impossible or involves a disproportionate effort'.
In accordance with the Regulation, personal data have to be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date (all reasonable steps should be taken to ensure that data which are inaccurate or incomplete in relation to the purposes for which they are collected or for which they are further processed, are erased or rectified);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or for which they are further processed.

Citizens enjoy legally enforceable rights under the Regulation, such as the right to access, rectify, block or delete personal data relating to them in files held by the Community institutions and bodies.

USA protection of personal data in EPRs - Health Insurance Portability and Accountability Act

US courts have found physicians liable for unauthorized release of medical information through the concept of a fiduciary duty of confidentiality in the physician-patient relationship.[20] Physicians who reveal a patient's personal information to third parties without appropriate justification may be liable for damages if the patient experiences harm as a result of the disclosure. Breach of confidentiality has also been recognized as a malpractice offence because it violates a professional standard of care.[21]

In the United States, a variety of state and federal statutes and common law rules establish legal obligations of physicians to protect patient confidentiality. Many medical licensing statutes include clauses that identify disclosure of medical information as a type of unprofessional conduct. Statutes in a majority of states also grant testamentary privilege to the physician-patient relationship; this privilege allows defendants to constrain physicians from disclosing patient information in a trial or other legal proceeding. In addition to these more general statutory protections, other statutes create special confidentiality protections for specific conditions. Among the conditions granted such protection are alcohol and drug abuse and HIV/AIDS.[19] Federal statutes also provide protection for health information, including information held by federal agencies, by health care institutions operated by the federal government, and by health care institutions participating in Medicare, Medicaid, and other federal health care programs.[21]

Potential threats to patient confidentiality from electronic health care transactions were implemented under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The American "Health Insurance Portability and Accountability Act" of 1996 mandated the development of standards to protect the confidentiality and security of patient medical records.[22] Health Insurance Portability and Accountability Act, was the first national legislation to assure every patient across the nation protection of their health insurance information. Hospitals and providers may use this information only for treatment, obtaining payment for care, and for specified operational purposes like improving quality of care. They must inform patients in writing of how their health data will be used; establish systems to track disclosure; and allow patients to review, obtain copies, and amend their own health information. HIPAA established standards and requirements for the electronic transmission of certain health information (eligibility requirements, referrals to other physicians, and health claims)[23] HIPAA protects a patient's rights to the confidentiality of his/her medical information and, for the first time, creates federal civil and criminal penalties for improper use or disclosure of protected health information.

Basic identifiers of the patient's past, present, or future physical or mental health conditions, including the provision of health

services and payment for those services must be confidential. Patients may understand and control how their health information and insurance is used or shared.[23, 24]
Healthcare providers who transmit health information electronically and even paper format, health plans, and healthcare clearinghouses are required to have a contract with the agencies they do business with so that they would comply with HIPAA regulations. According to Waldo[25] HIPAA regulations outline four general compliance issues that require organizations to have:

1. Policies and procedures to govern confidentiality, data integrity, and access.
2. Physical safeguards to control access and protect computers system against fire and other disaster.
3. Technical security measures to protect data held in information systems.
4. Technical security measures that protect and prevent interception and access to information sent via network.

HIPAA regulations, require providers to protect the confidentiality, integrity, and availability to patients of ''individually identifiable personal health information'' in any form, whether electronic, written, or oral. Personal health information includes information that relates to a person's physical or mental health, the provision of health care, or the payment for health care. The regulations apply to all health care organizations, including hospitals, physicians' offices, health care plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems, and ''any person or organization who furnishes, bills or is paid for health care in the normal course of business.''

For disclosures made in error, the HIPAA regulations assess civil penalties of US$100 per violation up to a maximum of US$25,000 per year. Although patients cannot sue privately for a HIPAA privacy violation, the Office of Civil Rights of the Department of Heath and Human Services is responsible for overseeing and enforcing the privacy regulations. Maximum criminal penalties for egregious violations include US$5,000 and 1 year's imprisonment for wrongful disclosure, US$100,000 and 5 years' imprisonment for disclosure under false pretences, and US$250,000 and 10 years' imprisonment for disclosure for profit or malice. In the first year of implementation of the HIPAA privacy rule, the Office of Civil Rights received more than 5,000 complaints of infractions and referred several dozen cases to the Department of Justice for prosecution.[26]
The Joint Commission on Accreditation of Healthcare Organizations (JCAHO), the recognized accreditation agency for US hospitals, has adopted explicit standards requiring respect for patient confidentiality and privacy. Although not legally required, JCAHO accreditation is a practical necessity for most hospitals. Failure to meet established JCAHO standards may jeopardize a hospital's accreditation. The 2003 JCAHO standards on Patient Rights and Organization Ethics include this statement: ''The hospital demonstrates respect for the following patient needs: confidentiality; privacy;''[27]

Greek institutional frame of safety - The constitutional consolidation of protection of personal data

At the last revision of Constitution was imposed the consolidation of a new, special right of protection of personal data. The new article 9[A] of Greek Constitution 1975/86/01 that was included in the Constitution in the last revision in 2001 defines that «everybody has the right of protection of its personal data from the collection, treatment and use, particularly when done with electronic means ». In the new provision it is described however the intensity of dangers that includes the process of data with electronic means. The protection of personal data belongs in the category of new rights that guarantee the revised Constitution. As this right is corruptible in offences from private individuals, the state cannot be satisfied by the dissuasion of these offences from his bodies, but it should take measures for this aim. The foundation of independent bodies is impressed as innate characteristic of system

ISSN:1108-7366, E-ISSN:1791-809X

for the protection of personal data in international texts, binding or not.[28, 29]

Law 2472/97 on the protection of personal data

Greek law 2472/97 establishes the Community Directive in the internal right and it simultaneously achieves the obligation of Greece that arises from the Constitution of 108 Council of Europe to establish special provisions on the protection of personal data. According to the European Directive 95/46/EK - and Greek law 2472/97- the use of medical data must be made under special regulations. According to the law 2472/97, when the sensitive personal data o each patient is used, the patient has the right:

- To be informed for the information from his file that are going to be used
- To be informed for the purpose of their use and which are going to have access and for how long.
- Ask the correction, or not to use part or all data.

While the obligations of persons in charge for the treatments of data of personal character are the following:

- Notify the Body of Protection of Data of Personal Character about the constitution and operation of such files that have sensitive personal data while in certain cases relative authorization is required.

Discussion:

The twentieth century is characterized by a revolution in provision of health care services. Advances in medical science and management have created an entirely new system of health care. People are not cared for by a single physician any longer. Instead, it is a collective process that includes nurses, many consulting physicians, laboratory technicians, diagnostic technologists and administrative staff. Moreover, a patient is no longer treated by one organization. A person can be admitted to one facility, transferred to another for treatment, and then require extended or home care. Therefore, it is necessary to uniquely identify patients across multiple providers and be able to access their information from multiple locations in order to support continuity of care.[30]

It is well known that EPR is indicative of the advances in medical informatics and allows providers, patients and payers to interact more efficiently. It offers new methods of storing, manipulating and communicating medical information of all kinds, including text, images, sound, video and tactile senses, which are more powerful and flexible than paper based systems but it poses moral and ethical dilemmas to the health care providers by the improper use of personal sensitive data of their patients.[31] In the healthcare environment privacy is particularly important since it enables collaboration between different data owners.[32]Clinicians in all European countries share the view that their responsibility to protect personal data in the health record extends to both manual and electronic records. By any chance revelation of this data places at risk the relationship between the health care provider and the patient which may be critical to the maintenance of public health. [33,34,35] Attention must also be given to how national laws are to be applied in situations where health data are processed in, or transferred between, more than one state. A code of conduct for the protection of personal health data, taking into account the E.U Directive and national laws, as well as ethical codes in each E.U country should be published widely among the health professions in order to encourage local enforcement and further harmonisation between countries. Research on breach incidents in health departments that are under the HIPAA rule found that during the previous year the names, birth dates, Social Security numbers, and disability ratings in some cases of as many as 26.5 million veterans were stolen recently from the home of a Department of Veterans Affairs employee. This theft represents the biggest unauthorized disclosure of Social Security data ever.[36] In 2005 a national Consumer Health Privacy Survey was conducted to unveil the impact of HIPAA Privacy Rules on consumers' attitudes towards and behaviours around personal health information. 2100 US adults responded to this research and the results showed that despite new federal

ISSN:1108-7366, E-ISSN:1791-809X

protections, consumers were still anxious about the privacy of their personal health information and misinformed about their rights under HIPAA.[37] In another 2005 (P&AB and Harris Interactive) survey, the results indicate that the serious concern almost suppresses the benefits of EPR.[32]:
- 70% of the people surveyed are concerned that personal health information could be disclosed because of weak data security
- 69% concerned that an EPR system could lead to more sharing of health information without patients' knowledge
- 47% report that privacy risks outweigh the benefits of EPR

The TA-SWISS study[38] on computer based Patients' Records mentioned that their uptake might result in the patients losing trust in health professionals, because they might feel that their privacy has been compromised.
The protection of electronically stored health data is important for Danish citizens also, as shown by the results of a Danish citizen's conference being held in 2002 for the EPR. The citizens approved that data in EPR is used for research and statistics, but it should be rendered anonymous. And they argue for a code of ethics and discipline in the use of EPR data in research. In Denmark, the citizens who participated in conference under the same theme, mentioned that existing legislation concerning patients' legal status and protection of personal data maintained in an EPR should be respected, and that he rules for informed consent and the legislation for protection of patient rights.[32] As we have seen above most European countries have relevant legislation, which guarantee data protection and data safety of patients. These, must certainly be maintained, if not reinforced.[32] While technological developments related to EPR have moved rapidly, and countries in E.U but in USA as well have legislated problems are still faced and EPR face a slow and sometimes difficult implementation. It is essential that governments develop compatible policy responses to ensure public confidence in the adoption of EPRs and interoperable EPR systems.[39] It is obvious that patients' right for the protection of his personal data can not be undermined by the use of an EPR. Vigilance, continuous control, sensitization of users and the reception of suitable, efficient, reasonable and economically bearable measures can ensure the confidential use of personal sensitive data.[30] The citizens prefer services and information adapted to their needs and their requirements, knowing that their right for privacy of their personal life is protected.[40]

Bibliography

1. Erickson J, Millar S. (2005).Caring for patients while respecting their privacy: renewing our commitment. Online Journal of Issues in Nursing. Available at http://nursingworld.org/ojin/topic27/tpc27_1.htm Accessed March 20, 2007.
2. Pownser SM., Wyatt JC, Writh P. (1998).Opportunities for the challenges of computerisation. Lancet 352: 1617–1622.
3. Barrows RC, Clayton PD. (1996). Privacy, confidentiality and electronic medical records. J. Am. Med. Inform. Assoc. 3:139–147.
4. Wyatt JC. (1994). Clinical data systems 2: components and techniques. The Lancet 344:1609–1614.
5. Malliarou M. (2007). Security policy and guarantee of medical secrecy of electronic patient record. Master thesis National Kapodistrian University of Athens, Nursing Faculty, Athens.
6. Younger K. (1972). Report of the Committee on Privacy to the UK Parliament, chaired by K. Younger, Cmnd 5012, HMSO, London.
7. Lindop N.(1978).Report of the Committee on Data Protection to the UK Parliament, chaired by N. Lindop, Cmnd 7341, HMSO, London.
8. Computers and Privacy, UK Parliament White paper. (1975). Cmnd 6353, HMSO, London.
9. Council on Scientific Affairs. (1993). Confidential health services for adolescents. Journal of American Medical Association 269: 1420-1424.
10. Annas GJ. (1993). Privacy rules for DNA databanks: protecting coded future

diaries. Journal of American Medical Association 270: 2346-2350.
11. European Official Journal (European Parliament). (1990) Directive on personal data protection. EEC: Brussels.
12. Council of Europe 1950: Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, and Protocols, Strasbourg, ISBN 92 871 0064 0.
13. Council of Europe 1981: Convention For the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, January 1981, ISBN (1982) 92-871-00225.
14. Council of Europe: Recommendation, R (81)1. (1981). On Automated Medical Data Banks, Strasbourg.
15. Council of Europe Recommendation, R (97)5. (1997). On the Protection of Medical Data, Council of Europe, Strasbourg.
16. European Community Directive 95/46/EC. (1995). 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.
17. Louveaux P. (1995). Data Protection in Health Telematics Projects: Compliance with the European Directive on the Protection of Personal Data.
18. Clark R. (1996).Implications of the E.U Data Protection Directive and Council of Europe Recommendation for HCEs, ISHTAR consortium deliverable ref I04UDOIA.
19. Barber B. et al. (1997).The definition of data privacy for Europe, in HC97 current perspectives, in: Richards et al. (Eds.), Health Care Computing 1997, pub for BCS by BJHC Weybridge, pp. 47–54, ISBN 0 948198 26 5.
20. Liang BA. (2000).Medical information, records, and confidentiality. In: Liang BA, ed. Health Law and Policy. Boston, MA: Butterworth- Heinemann: 45-62.
21. Roach WH. (1998). Medical Records and the Law. 3rd ed. Gaithersburg, MD: Aspen Publishers: 98-102.
22. US Department of Health and Human Services, Office for Civil Rights. Summary of the HIPAA privacy rule. Available at: http://www.hhs.gov/ocr/privacysummary.pdf. Accessed February 2, 2007.
23. American Hospital Association. (2002). HIPAA Privacy Standards. Available in www.hospitalconnect.com/hospitalconnect/jsp/keyissues.jsp?topic=HIPAA. Accessed January 21, 2006.
24. Amatayakul, M. (2000). Achieving compliance with the new standards. MD Computing. 54-56.
25. Waldo H. (1999). Managing data security: developing a plan to protect patient data. Nursing Economics. 17(1) 49-53.
26. Finkelstein JB. One year later, mixed reviews for privacy rule. Available at: http:// www.ama-assn.org/amednews/2004/05/03/gvsc0503.htm. Accessed June 28, 2006.
27. Joint Commission on Accreditation of Healthcare Organizations. (2003). Comprehensive Accreditation Manual for Hospitals. Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations: I-15.
28. Fowles JB, Kind AC, Craft C, Kind EA, Mandel JL, Adlis S.(2004). Patients' interest in reading their medical record: relation with clinical and sociodemographic characteristics and patients' approach to health care. Arch Intern Med 164(7):793-800.
29. Ross SE, Moore LA, Earnest MA, Wittevrongel L, Lin C. (2004). Providing a web-based online medical record with electronic communication capabilities to patients with congestive heart failure: randomized trial. J Med Internet Res 6(2):e12.
30. Office of Health and the Information Highway Health Canada. (1998). International Activities. Toward Electronic Health Records: Unique Identification and PKI. Available at: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/1998-ehrdse-int/index_e.html#top Accessed March 15 2007.
31. Electronic Patient Records.2000 Simon Rogerson Originally published as ETHIcol in the IMIS Journal 10;5.
32. Web site. Available at: www.srdc.metu.edu.tr/webpage/projects/saphire/deliverables/SAPHIRE%20Privac

y%20Sensor%20D6-2Interim.doc Accessed March 12 2007.
33. Parker D. (1984). The many faces of data vulnerability, IEEE Spectrum 5:46–49.
34. Lance JE. (1992). Keeping the lid on secrets. Risk Management: 39:18.
35. Wiant T. (2005).Information security policy's impact on reporting security incidents. Computers & Security; 24(6):448-459.
36. Survey on data security breach discloses veterans' medical information. (2006). Available at: www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=374199 Accessed May 12, 2007.
37. Bishop L, Holmes B, Kelley C. (2005). National Consumer Health Privacy Survey. California HealthCare Foundation Oakland. Available at: www.chcf.org Accessed May 12, 2007.
38. Available at: http://www.taswiss.ch/wwwremain/reports_archive/publications/2004/040924_TA_49A_e_definitiv.pdf Accessed May 20 2007.
39. The Diebold Institute for Public Studies, Inc. Healthcare Info structures: The Development of Information-Based Infrastructures for the Healthcare Industry. (1995).A focus on the role that information-based technology can play in improving overall health and well-being in U.S. society.
40. Pangalos G. (1992).Security in medical database systems in EEC, SEISMED project report no. INT/S.3/92.

ISSN:1108-7366, E-ISSN:1791-809X