MEDINFO 2001
V. Patel et al. (Eds)
Amsterdam: IOS Press

Info-Vigilance or Safety in Health Information Systems

Barry Barber[a], François-André Allaert[b], Eike-Henner Kluge[c]

[a] *Health Data Protection Ltd, Great Malvern, England*
[b] *Managing Director of CENBIOTECH, Dijon, France*
[c] *University of Victoria, Canada*

Abstract

The paper examines the issues of security and safety in Health Information Systems and focuses the need for the development of appropriate Guidelines for the effective use of IEC 61508 standard.

Keywords:

Safety, Guidelines, Standards, Info-vigilance, IEC61508

Introduction

Safety-Related Systems

In the late 1980s and early 1990s there arose considerable concern about the use of systems and software to control dangerous processes for nuclear reactors, air traffic and the like. This concern was reflected in a joint study report prepared by the Institution of Electrical Engineers and the British Computer Society [1]. This book includes other material on safety-related systems such as the DRIVE Report, which reviewed current tools and techniques for the development of safety-critical software. It, also, provides an overview of the education and training of safety-critical systems practitioners and defence standard 00-55. The concern was shared by the UK Department of Trade and Industry, which set up and co-ordinated Safety-Critical Systems Club to examine these issues. Redmill and Rajan [2] outline the progress that has been made in understanding the issues involved over the last decade.

Safety in Medical Informatics

Concern over safety was not limited to these areas. During the first phase of the Advanced Informatics in Medicine programme of the European Union, consideration was given to the future in the context of the "Impact Assessment and Forecast" study. This work, published by Roger-France and Santucci [3], developed the idea of regulating Health Telematics according to "Six Safety First Principles". These were elaborated by Barber, Jensen, Lamberts, Roger-France, de Schouwer & Zöllner [4]. The study group was surprised to find the issue of safety arising at this stage because it was confidentiality and not safety that had been the main previous focus of discussions of problems in medical informatics. In retrospect, however, it should not have been surprising since already the Hippocratic Oath states that "I will help the sick according to my ability and judgement but I will never use it to injure or wrong them;" and, again that "I will not use the knife either on suffers from stone but I will give place to such as are craftsmen therein" [5]. These clauses clearly place the issue of safety at the centre of medical concern. Traditionally, security has been concerned with the confidentiality, integrity and availability of information and the accountability for it. Safety has been concerned with wider issues of the overall effect of the use of various systems and generally, the development of standards has been sector specific. In Healthcare the issues of safety and security need to be brought together.

Security in Medical Informatics

Within the English National Health Service [NHS], the implementation of the Data Protection Act 1984, based on Council of Europe Convention 108 [6], led naturally to an examination of the appropriate security measures as required by Article 7. A variety of Risk Analyses were undertaken within the NHS utilising the CCTA Risk Analysis and Management Methodology [CRAMM] which was the UK government's own approach to elucidating these issues [7]. In this methodology, problems arising from security breaches were measured in a variety of dimensions but the most interesting from the Healthcare standpoint were the dimensions of financial loss and of damage or death of patients. Significantly, this work called for much more stringent security measures to cope with safety issues than had normally been practiced for purely financial or confidentiality reasons [8].

Within the UK, this work had the effect of raising the issues of the integrity and availability in respect of the use of electronic medical records on the basis of the government's own risk analysis methodology. These considerations were based around the development of "worst case scenarios". *"They must not stretch the bounds of credulity but rather represent the a view of events that might be foreseen and expected to happen in particular circumstances by a*

reasonable person - not every time, not necessarily most times, but from time to time" [9]. In a very real sense the development and maintenance of these worst case scenarios raised major clinical and managerial issues: What would a reasonable person expect to happen in the event of a breach of security? What would such a person, or a court of law, regard as negligence?

What Has Gone Wrong?

In order to give appropriate answers to these questions, it is important to have some understanding about actual situations where things have gone wrong. However, it is not easy to do this. Many organisations are unwilling to provide access to critical incidents for fear of laying themselves open to legal action and/ or causing an exodus of their patients which could affect their financial viability. This is particularly true when fatalities or serious injuries are involved. Unfortunately, therefore, the most frequent access to reports of such failures is through the press. While such reports provide useful material for training purposes, it is rare that they allow one detailed insight into the facts of the case. Further, since they normally give a journalist's hurried view of a situation, the information they present may well turn out to be wrong when the full facts are reviewed subsequently.

The safety-related literature usually holds up the case of the Therac 25 linear accelerator as the best example of a serious breach of Healthcare safety arising from an integrity failure. It is referred to by Redmill and Rajan [2 p 240] and is extensively covered by Peterson [10]. In this instance, there were 6 radiation accidents involving substantial overdoses that led to at least 4 deaths. These accidents were caused by a "complex web of interacting events with multiple contributing technical, human and organisational factors". Correspondingly, the under-dosage reported at the North Staffordshire Royal Infirmary also appears to have arisen from a multiplicity of interacting factors [11]. Another example - the computer project problems of the London Ambulance Service - have been reported in detail by Beynon-Davies [12]. They were blamed for 20 - 30 deaths as a result of the non-arrival of urgently required ambulances. Another case reported at Arrowe Park Hospital on the Wirral [13] involved the modification of patient data. . In this case, a nurse was convicted under section 3 of the Computer Misuse Act 1990 with unauthorised modification of computer material and sentenced to 12 months in prison. The prescription record of a 9 year old was changed to a potentially lethal cocktail of atenol, temazepam, benzoflumethiazide and coproxamal. Fortunately, this modification was noticed and not acted upon by the ward sister.

Other examples include press reports of medical records ending up on rubbish dumps and on obsolete computers sold on to the public, theft of medical systems containing patient data, private investigators being able to get medical records for specific individuals at will, medical databases being hacked into, losses of medical records, especially research studies, poor software in medical systems and virus infections. The ISHTAR project [14] attempted to establish a database of Healthcare Security Incidents but, although it did develop a Healthcare Incident Reporting Scheme, the Verification Centres of the project were unwilling for their incident reports to be shared.

In addition, there are press reports of medical errors concerning inappropriate treatments that sometimes lead to the death of patients: errors that arise from illegible writing, incorrect drug administration, incorrect prescribing, incompatible blood transfusion, misinterpretation of laboratory tests, incompetent surgery, etc. All of these indicate areas in which security breaches in respect of the patients' medical records might lead to serious harm to patients as a result of reliance on the validity of the patients' records.

How Safe Should Medical Systems be?

In light of the preceding, it is appropriate to ask how safe medical practice should be. On the one side, there is the fact that one paper reported that a review of five years work of one particular pathologist's "mis-diagnosis" had found 186 errors in 12,000 cases reviewed [14]. More recently, another pathologist claimed that he had an error rate of "no more than 2%, which was average in the UK and better than many doctors abroad. Internationally, the incorrect diagnosis rate varies from 2% to 7%". A review of 10,358 of his cases found 7 patients with a wrong diagnosis that had serious consequences, and 215 cases whose histology had to be revised [15]. In both these cases, the pathologists were considered to have a bad performance record. However, by contrast, it should be noted that in most occupations an error rate of around 2% would be considered good. These figures indicate just how great are our expectations of medical systems.

Recently, the BMJ devoted an edition to the issues of Reducing Error and Improving Safety that was introduced by an editorial by Leape and Berwick [17]. They noted that a recent report from the Institute of Medicine [18] had given a great impetus to the examination of safety issues in medicine in the USA, and that Weingart SN, Wilson RM, Gibberd RW and Harrison B [19] had provided comparable results from Australia. Barach and Small [20] examined the characteristics of error and near-miss reporting schemes in other sectors to see what light they might shed on the schemes that need to be developed for the Healthcare sector. Reason [21] explored the permanence of human fallibility and the need for the development of a systems approach within which error-prone humans can work and still achieve highly reliable results.

However, the overall conclusion to be drawn was that there needs to be a major change in culture to support confidential incident reporting arrangements that will actively seek out and rectify the causes of safety failures. In order to reduce error rates, the culture in which healthcare is delivered, the design of activities and processes and the training of practitioners will all have to change. In fact, the problem is not seen as the fundamental lack of knowledge so much as the lack of a supportive

environment within which physicians can report errors and learn, collectively, from their mistakes thus leading to improvements in patient safety.

Developments in Healthcare Systems

It is at this juncture that safety in informatics becomes relevant. Information systems have been utilised in the various processes of delivering Healthcare for some four decades. However, it is only recently that such systems have been applied to analyse and critique the processes of delivering care. There are now more Health-related Information Systems, more Health Professionals using these systems, more non-Health Professionals using these systems, more critical medical systems being used, more reliance on the Information Systems and more fragmentation in the Healthcare delivery arrangements than ever before. All these factors raise concerns that have to be addressed in respect of patient safety.

Of course, few Health-related Systems are set up so that they automatically decide on clinical treatment or drug dosage and then implement their decisions. In general, there is a Health Professional in the "air-gap" between the patient and the Information System. In theory, this gives the Health Professional total control of the diagnostic and treatment processes. However, the Health Professional may believe erroneous information provided by the system, may not have the specialist knowledge to validate the data or suggestions offered by the Information System, may be rushed or worried by many other professional and personal matters crowding onto his/her agenda and may not be working in a supportive clinical environment.

As a result he/she may fail to protect a patient from damage arising from erroneous information provided by the Information System. He/she may take undesirable therapeutic action from a mistaken belief in the accuracy of the information from the system or he/she may fail to take desirable therapeutic action for similar reasons. The closer that Health-related Information Systems come to the heart of the complex set of clinical processes, the more serious become the security and safety hazards associated with the use of such systems.

Another problem is presented by networked information systems. That is to say, Health Professionals increasingly need access to their systems when they are away from their desks – which of course means that access from remote locations must be possible. The technology can improve safety by access to information where this would not previously have been possible. However, this raises safety concerns that centre on the problem of unauthorised access to networked information systems. The lessons on the relative ease with which information systems may be attacked over a network have still to be learned and fully implemented [22].

IMIA and Safety

There were five papers at MEDINFO 74 associated with various aspects of Data Protection, and the early establishment of IMIA WG4 makes clear the importance that the International Medical Informatics Association has attached to these issues. Although the clinical issues were not seen as clearly then as they are now, the WG4 monograph [23] clearly raises the issue of "Data/program Integrity" and "Usage Integrity". The issues of integrity, availability and accountability have been fully woven into the five working conferences of IMIA WG4 [24 - 28] since that time - in addition to the more traditional issues of confidentiality.

Security Requirements of the EU Directive

The EU Directive "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data" [29] sets out specific requirements in respect of the security of personal data. These are that "the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing". The Directive, further, requires that "Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

These requirements are still clearly focussed on the data that are held in an information system and do not appear fully to take in the requirements for patient safety. However, they do go a long way in that direction. The data are clearly personal health data, and are therefore subject to special safeguards as special category data. In most systems, there will be data transmission over a network even where the application is not specifically one involving telemedicine. Where this system is closely coupled with the delivery of Healthcare, the risks will clearly involve patient safety. This means that security measures need to be up-to-date both in terms of technology and expense. However, it should be noted that that the Council of Europe Recommendation "On the Protection of Medical Data" [30] does not place quite the same emphasis on the cost issue.

Ethical Handling of Personal Health Data

In view of the fact that electronic patient records are increasingly being relied upon by the Health Professionals, and given that these records are increasingly being networked throughout the caring community, it is time to take a close look at the ethical rules that govern the actions of Healthcare information professionals. A number of ethicists have been doing this but Kluge has developed a set of "Fair Information Principles" that reflect best ethical practice.[27,31,32] These concepts have been developed over the last decade and are now reflected most extensively in a book [33]. It suggests that these Ethical Principles should govern the behaviour of Health Information Professionals, and that they require Health Professionals to take full account of the safety issues and utilise safe systems.

What Is a Medical Device?

The definition in the EU Directive [34] "Concerning Medical Devices" is tantalising in that it "means any instrument, apparatus, appliance, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of:-Diagnosis, prevention, monitoring, treatment or alleviation of disease; Diagnosis, prevention, monitoring, treatment or alleviation of or compensation for an injury or handicap; Investigation, replacement or modification of the anatomy or of a physiological process; Control of conception and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means". The accompanying definition of "accessory" identifies it as "an article which whilst not being a device is intended specifically by its manufacturer to be used together with a device to enable it to be used in accordance with the use of the device intended by the manufacturer of the device".

The wording appears quite wide, and the words "including software" and "accessory" raise the issue of the point at which a Health Information Systems becomes within the scope of the medical devices legislation. However, there are things to be learned from the medical devices legislation whether or not it is applicable in the strict sense. The legislation establishes a classification scheme for medical devices with increasingly stringent requirements for more risky devices. It establishes a monitoring scheme for collecting information on incidents relating to medical devices put on the market. The Directive makes clear reference to appropriate standards, and it establishes national bodies to oversee the legislation. In addition, there is a clear implication that a medical device shall be recognisable as having been put on the market by a "manufacturer" meaning "the natural or legal person with responsibility for the design, manufacture, packaging and labeling of a device before it is placed on the market". This implies that an information system would have to be identifiable and packaged rather than being purchased as a variety of hardware and software components for which no-one was taking overall responsibility.

The Next Steps in Standardisation

Curiously, safety and security in respect of information systems seem to be separate concepts in all areas except in the case of Healthcare. This may result from the fact that the focus of interest in Healthcare is that of patient safety, whereas confidentiality and financial loss, although very important, are not quite as central. However, complete and integrated standardisation is really necessary. The conventional UK approach to Information Security Management standards is from the standpoint of BS7799 [35] and the UK Data Protection Commissioner is currently looking for security at this standard. The next step is that of providing Healthcare specific safety guidelines for the use of the IEC 61508 standard [36]. This safety standard has been used successfully in a number of other sectors and, with the increasingly clinical and critical use of Health Information Systems, it is therefore time for that standard to be developed and utilised in Healthcare. The European standards body CEN TC 251 commissioned a technical report [37] which reviewed the various ways forward. CEN is only waiting for the opportunity to take this work forward into the formal standards arena utilising IEC 61508.

However, standards by themselves are not sufficient. Standards are only as effective as the people who apply them. Therefore we also need to establish

- A Safety Culture for Health Information Professionals to match the developing culture among Health Professionals
- A practical Code of Ethics for Health Information Professionals,
- Appropriate standards for developing and using safe Health Information Systems, and
- An international body empowered to supervise the application of the relevant codes and standards.

References

[1] Wichmann B A. *Software in Safety-Related Systems.* John Wiley for BCS, Chichester, 1992

[2] Redmill F and Rajan J. *Human Factors in Safety-Critical Systems.* Butterworth-Heinemann, Oxford 1997

[3] Roger-France FH and Santucci G. *Perspectives of Information Processing in Medical Applications.* Springer Verlag, Berlin 1991

[4] Barber B, Jensen, O A, Lamberts H, Roger-France, de Schouwer P & Zöllner H, The Six Safety First Principles of Health Information Systems: A Programme of Implementation, pp 608-619 in *MIE90* ed O'Moore R, Bengtsson S, Bryant J R & Bryden J S, vol 40 in Lecture Notes in Medical Informatics, Springer Verlag 1990

[5] Jones WHS. The Doctor's Oath, Cambridge University Press, 1924, pp 9 - 11

[6] Council of Europe 1981, *Convention For the Protection of Individuals with regard to Automatic Processing of Personal Data*, Convention 108, January 1981,

[7] The CRAMM User Guide, issue 1.0 April 1996, CRAMM software 3.0, The CRAMM Manager, PO Box 1028, London

[8] Barber B & Davey J, *The Use of the CCTA Risk Analysis and Management Methodology [CRAMM] in Health Information System's,* pp 1589 - 1593, in *MEDINFO 92,* ed Lun KC, Degoulet P, Piemme TE and Rienhoff O, pub for IMIA by North Holland, Amsterdam, 1992

[9] Barber B, Vincent R and Scholes M. *Worst Case Scenarios: the Legal Consequences*, pp 282 - 288, *HC 92: Current Perspectives in Healthcare Computing 1992*, ed Richards B, MacOwen H, Bryant JR, Gillies M, Hayes G, Jones R and Roberts J, pub for British Computer Society by BJHC Weybridge, ISBN 0 948198 12 5

[10] Peterson. P *Fatal Defect: Chasing the Killer Computer Bugs*, pp 27 - 48, Vintage Books, New York, 1995

[11] West Midlands Regional Health Authority, *Reports into the Conduct of Isocentric Radiotherapy at the North Staffordshire Royal Infirmary between 1982 and 1991*, Birmingham 1992 and 1994

[12] Beynon-Davies P, Information Systems "Failure": the case of the London Ambulance Service's Computer Aided Dispatch project, European Journal of Information Systems, 1995, 4, 171 - 184

[13] *Nurse Jailed for Hacking into Computerised Prescription System,* British Journal of Health Care Computing, p7, vol 11, February 1994

[14] *Implementing Secure Healthcare Telematics Applications in Europe – ISHTAR*, IOS Press, Studies in Health Technology and Informatics vol 66, Amsterdam 2001

[15] The Independent, 8 October 1994, London

[16] The Guardian, 15 June 2000, London

[17] Leape KK and Berwick DM, *Safe Health Care: Are we up to it?* BMJ, 2000;320:725 - 726

[18] Kohn LT, Corrigan JM, Donaldson MS eds, *To Err is Human. Building a Safer Health System*, National Academy Press, Washington DC, 1999

[19] Weingart SN, Wilson RM, Gibberd RW and Harrison B, *Epidemiology of Medical Error*, BMJ, 2000;320:774-777

[20] Barach P and Small SD, *Reporting and Preventing Medical Mishaps: Non-medical near miss reporting systems*, BMJ, 2000;320:759-763

[21] Reason J, *Human Error: Models and Management*, BMJ 2000;320: 768-770

[22] Stoll C, *The Cuckoo's Egg*, Pan Books, London, 1991, ISBN 0-330-31742-3

[23] 23] Griesser GG, Bakker A, Danielddon, Hirel J-C, Kenny D, Schneider W and Wassermann AI, *Data Protection in Health Information Systems: Considerations and Guidelines*, pp 53-55, North Holland, Amsterdam, 1980, ISBN 0 444 86052 5

[24] Griesser G, Jardel JP, Kenny DK & Sauter K, *Data Protection in Health Information Systems: Where Do We Stand?,* North Holland, 1983 Amsterdam, ISBN 0 444 86713 9

[25] Barber B, Bakker AR & Bengtsson S, *ed Caring for Health Information: Safety, Security and Secrecy,* International Journal of Bio-Medical Computing, vol 35, Supplement February 1994 Amsterdam,

[26] Bakker AR, Barber B, Pellikka RT K & Treacher A, ed *Communicating Health Information in an Insecure World*, International Journal of Bio-Medical Computing, vol 43, pp 1-152, Supplement October 1996 Amsterdam

[27] Bakker AR, Barber B, Ishikawa K & Yamamoto K, ed *Common Security Solutions for Communicating Patient Data*, International Journal of Bio-Medical Computing, vol 49, pp 1-137, Supplement October 1998 Amsterdam

[28] Bakker AR, Barber B, Moehr J, International Journal of Medical Informatics, vol 60, No 2, 2000 Special Issue: Security of the Distributed Electronic Patient Record

[29] 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*, OJ L281/31 - 50, 24 October 1995

[30] Council of Europe Recommendation, R(97)5, *On the Protection of Medical Data*, Council of Europe, Strasbourg, 12 February 1997

[31] Kluge E-HW, Medical Information & Education: The Profession or Gate Keeper, *Methods of Information in Medicine,* 28 (1989) 196-201

[32] Kluge E-HW, . Health Information, the Fair Information Principles and Ethics," *Methods Inf Med* 1994:33; 336-346

[33] Kluge E-HW, *The Ethics of Electronic Patient Records,* New York, Peter Lang (in press).

[34] 34] European Community Council Directive 93/42/EEC, *Concerning Medical Devices*, OJ L169/1-43, 12 July 1993

[35] British Standards Institution, BS7799, London 1999 Code of Practice for Information Security Management[Part 1] and Specification for Information Security Management [Part 2]

[36] International Standards Organisation/International Electrotechnical Commission, ISO/IEC *61508 IT Security Techniques - Evaluation Criteria for IT Security Functional Safety of electrical/electronic/programmable electronic safety-related systems Parts 1 to 7*

[37] Safety and Security Related Software Quality Standards for Healthcare (SSQS), CEN/TC 251/WG III N 98-036, 26 October 1998, Brussels.

Address for correspondece

Barry Barber, 12 Peterson Court, Worcester Road, Great Malverm, Worcs, England barry@healthdataprotection.ltd.uk