The application of the FMEA risk assessment technique to electronic health record systems

Khin Than Win
University of Wollongong

The Application of the FMEA Risk Assessment Technique to Electronic Health Record Systems

A thesis submitted in partial fulfilment of the
requirements for the award of the degree

Doctor of Philosophy

from

University of Wollongong

by

Khin Than Win
M.B.B.S, DCS, IDCS, MS-CIS

School of Information Technology and Computer Science
2005

Declaration

I, Khin Than Win, declare that this thesis, submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Information Technology and Computer Science, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

Khin Than Win
May 2005

ABSTRACT

Patient safety and Medical errors are of growing concern in the health care industry. Some errors are caused by preventable adverse events; identifying potential errors and preventing them would mitigate risk and hence enhance the safety. Electronic health records (EHRs) are an inherent part of the healthcare systems and thus it is imperative that errors do not originate from EHRs.

A thorough literature review indicated that *no* risk assessment methods currently exist for EHR systems. Project management risk and system security risk assessments do exist but not risk assessment of threats to safety. Accordingly, this research aims to develop a framework for the safety and dependability of EHRs, in order to analyse the risks associated with electronic health record systems.

This research has identified a relationship of dependability and data quality of EHRs and attributes for the safety assessment of EHRs. The research involved (i) developing a theoretical basis of safety, based on dependability and data quality, (ii) defining the safety attributes of EHRs, (iii) identifying the risk assessment method applicable to EHRs, and (iv) conducting case studies of EHRs in different healthcare settings.

A thorough understanding of EHRs is important to identify safety attributes of EHRs. Therefore, different EHRs, EHR systems around the world - their purposes, functionalities and information management - are all explored.

This study investigated different available risk assessment methods and analysed them against different case scenarios to determine the appropriate risk assessment method for EHRs. After careful consideration, Failure Mode Effect Analysis (FMEA) was identified as an appropriate method for EHRs risk assessment.

The idea and concept of risk assessment of EHRs were investigated by empirical studies on (i) the Community Health Information Management Enterprise (CHIME), Illawarra Area Health Service, and (ii) Maternal and Infant Network (MINET) database, South Western Sydney Area Health Service.

Results from the case studies indicated that safety attributes identified from this research are appropriate for EHRs and that FMEA is indeed a suitable risk assessment method for EHRs. This study has verified by case studies that data availability, reliability and security are all important for safety. Potential systems risks- such as patient misidentification, security breaches due to initial password, and incorrect linkage of data were identified from this research and notified to the appropriate personnel such as system administrators and health care providers. Improvements to the systems in question have been achieved through modifications based on the results uncovered from these case studies. It can be concluded that the safety attributes identified from this research are essential for the safety of EHRs. It was also discovered that system quality is just as important, and therefore should be included in any safety assessment of electronic health record systems. It was further found that the safety cultures of

organisations and healthcare providers are important in conducting risk assessment of EHRs.

Publications from this Thesis

1. **Win K.T**., Croll P. (2005), Engineering Dependable Health Information Systems, In: Creating knowledge based healthcare organization, editors: Wickramsinghe N., Gupta J.N.D., Sharma S. K. Idea Group Publishing, pp 91-109
2. **Win K.T.(**2004), Identifying the risk assessment method applicable to the electronic health record systems, Proceedings of HIC2004, Brisbane, July 25-27
3. **Win K.T.,** Cooper J., Alcock C. (2004), Risk assessment of electronic health record system, Proceedings of CollECTeR2004 Workshop, Adelaide, May 7-8
4. **Win K.T**., Croll P., Cooper J. (2002), Introducing Risk Assessments to Electronic Medical Record Systems, Proceedings of Second International Conference on the Management of Healthcare and Medical Technology on: The Hospital of the Future, Chicago, Illinois, USA, July 28-30, 2002
5. **Win K.T**., Croll P., Cooper J. (2002), Setting a Safety standards for electronic medical records, Proceedings of HIC2002, The Tenth Annual Health Informatics Conference, Melbourne, Australia, August 4- 6.
6. **Win K.T,** Phung H, Young L, Tran M, Alcock C, Hillman K. (2004), Electronic Health Record System risk assessment: a case study from the MINET, Health Information Management Journal, vol.33, is. 2, 43-48

II. Other Related Publications by this author

7. **Win K.T**., Croll P., Cooper J., Alcock C. (2002), Issues of Privacy, Confidentiality and Access in Electronic Health Record, Journal of Law and Information Science, vol.12, is.1, pp 24-45
8. Phung H, Young L, Tran M, **Win K.T**. (2004), Alcock C, Hillman K., Health informatics and health information management in maternal and child health services, Health Information Management Journal, vol.33, is. 2, pp 36-42
9. **Win K.T.,** Cooper J. (2004), Information Age, Electronic Health Record and Australia Healthcare, International Journal of Computer Internet and Management, Special Issue on Managing Healthcare Science And Technology For Effective Delivery (in press)
10. **Win. K.T** (2005), Web based personal health record systems evaluation, accepted for the Special Issue on "The application of Internet-based information and communication technologies to healthcare", International Journal of Healthcare technology Management" (in press)
11. Alcock C., Burgess L., Cooper J., **Win K. T**.(2004), Electronic Health Systems: Integration of Inconsistent Information in Heterogeneous Multidatabase Health Systems, Proceedings of CollECTeR LatAm 2004, Santiago, Chile
12. **Win K.T**., Cooper J., Croll P., (2003), Engineering Pragmatic Patient Consent in Electronic Health Record Systems, Proceedings of World

Congress on Medical Physics and Biomedical Engineering 2003, Sydney, Australia August 24-29

13. **Win K.T.,** Croll P., Cooper J., (2003), Dependability: Important factor for the success of electronic health record systems, Proceedings of The eleventh Annual Health Informatics Conference, Darling Harbour, Sydney, Australia, 10 –12 August
14. **Win K.T.**, Croll P., Cooper J., (2003), Privacy, confidentiality and consent of electronic health record systems, Proceedings of The eleventh Annual Health Informatics Conference, Darling Harbour, Sydney, Australia, 10 –12 August
15. **Win K.T**., Song H., Croll P., Cooper J. (2002), Implementing patient's consent in electronic health record systems, Proceedings of CollECTeR 2002, Melbourne, Australia., December 1, 2,2002
16. **Win K.T**., Croll P., Cooper J., Alcock C. (2001), Issues of Privacy, Confidentiality and Access in Electronic Health Record, In: Proceedings of Information Technology and Emerging Law, Wollongong, September 28.
17. **Win K.T.**, Selakovic G. (2004), Evaluative study of Web Based Personal Health Record Systems, Proceedings of CollECTeR2004 Workshop, Adelaide, May 7-8
18. Song H., Croll P., **Win K.T**. (2003), A Prototype of Patient e-Consent in Access Control to Electronic Medical Records, Proceedings of Asia-Pacific Association of Medical Informatics (APAMI) conference, Korea

19. Song H., **Win K.T**., Croll P.(2002), Patient e-consent mechanism: Models and Technologies, Proceedings of CollECTeR 2002, Melbourne, Australia., December 1, 2,2002
20. Fuller A., **Win K.T**, Di L. (2002), Experiences using case studies to teach risk, Proceedings of 32nd ASEE/IEEE Frontiers in Education Conference, Boston, November 6-9
21. Alcock C., Burgess L., Cooper J., **Win K.T**. (2001), The Rise of E-health in Australia: Electronic Health Records and Privacy Legislation. In; Proceedings of the Fourth International Conference on Electronic Commerce Research (ICECR -4). Dallas, Texas, USA. November 8-11, vol.2, pp 466-474

Acknowledgement

I would like to extend my heartfelt gratitude and appreciation to my Supervisor Professor Joan Cooper for her invaluable guidance and support throughout the course of this research for my Ph.D. degree. My sincere thanks and appreciation go to Professor John Fulcher for assisting me and guiding me through the thesis in the final stage. I am also indebted to Associate Professor Carole Alcock for her assistance in the final stages of preparation of this thesis.

I highly value the assistance of Dr. Hai Phung and the staff of Simpson Center for Health Services Innovative Research for helping me in collecting information for the Risk Assessment of the Maternal and Infant Network (MINET). I also wish to convey my thanks to Mr. Shane Simpson and the staff involved in Community Health Information Management Enterprise (CHIME), Illawarra Area Health Service for their time and for providing information for the risk assessment study of CHIME.

My deep gratitude goes to my parents and brothers for their encouragement and inspiration in all my undertakings. I would also like to express my love and gratitude to my husband Liming Qiang for his support and patience during this study. Finally, I would like to dedicate this thesis to my son Vincent, my pride and joy, who was born during the course of this work.

Table of Contents

Tables

Figures

CHAPTER ONE

FRAMING THE RESEARCH PROBLEMS

1.1. Statement of the research problem

In, "To Err is Human: Building a Safer Health System", Kohn et al. highlighted the importance of safety and quality of healthcare:

> *"At least 44,000 people, and perhaps as many as 98,000 people, die in* (United States) *hospitals each year as a result of medical errors that could have been prevented, according to estimates from two major studies. Even using the lower estimate, preventable medical errors in hospital exceed attributable deaths to such feared threats as motor-vehicle wrecks, breast cancer, and AIDS"* (Kohn et al. 2000).

Medical errors are of growing concern in the health care industry. As electronic health records (EHRs) are now part of the healthcare system, a necessary requirement is that EHRs are safe and dependable. Dependable electronic health record systems could help reduce the risk of occurrence of medical errors.

1.2. Research questions:

This research therefore aims to develop a framework for the safety and dependability of the EHRs in order to analyse the risks associated with electronic health record systems. More specifically,

1. How can the safety of EHRs be measured? and
2. What are the safety attributes of EHRs?

1.3. Research Approach

The research will define a model of dependability that works for EHRs. Safety is one of the subsets of dependability; dependable systems ensure data quality. EHRs involve different processes, from data entry to decision-making. Establishing a relationship framework for dependability, data quality and EHRs would assist in identifying safety requirements.

Therefore, a framework for safety assessment of EHRs is developed by

- Examining the concept of 'safety';
- Describing risk assessment techniques
- Identifying a risk assessment method applicable to EHRs,
- Applying this risk assessment method to two cases, and
- Drawing conclusions about the effectiveness of that risk assessment technique in achieving the declared objectives

Risk assessment case studies will be conducted in two different health care institutions' EHRs after identifying the appropriate risk assessment method from this study. Case studies will be conducted to validate whether the identified risk assessment methods can be applicable to the safety assessment of EHRs.

1.4. Significance of the research

Identification of safety requirements of EHRs would help to reduce errors by being able to mitigate the risk of error occurrence. Dependability, safety and risk are defined and explained in Chapter Four. Exploring undesirable events that can occur from electronic health record systems would assist in identifying risk.

Different risk assessment methods are available for different systems. This research identifies the appropriate risk assessment method applicable for EHRs. With the proper risk assessment, risk can be identified and minimised so that there will be safer health record systems, leading in turn to a safer healthcare system. Awareness of risk and safety requirements is important as that would assist in reengineering of the appropriate EHRs for various health care organizations.

The research is timely with requirements having been set by most countries for full implementation of EHRs (Carnall 1998; NEHRT 2000) and looking into the safety of the health care systems (Kohn et. al. 2000; Institute of Medicine 2001; Battles and Lilford 2003). The issue of patient safety has been focused in Australia (Safety and Quality Council 2003), the United States of America (Kohn et. al. 2000; Institute of Medicine 2001), Great Britain (Department of Health 2000) and Europe (Brunner et.al. 2001). There is a belief that computer-based health record systems would improve quality and efficiency of patient care (McDonald 2002); risk assessment is needed to ensure that EHR systems are safe.

There are numerous examples from other industries, where safety is important and failure to comply with standards has the potential to have an immense impact on human life - for example, air traffic control and railroad monitoring systems. In the healthcare industry, medical radiation systems, ECG monitoring systems and insulin infusion pumps are all examples of safety systems. Such systems

need to follow the relevant safety standards. Similarly, development of EHR systems needs to follow the standard specified for EHRs.

A thorough literature review has revealed a lack of comprehensive studies relating to the safety and dependability of EHR systems. Accordingly, risk assessment of the EHRs emanating from this study contributes to the building of safer health information systems.

1.5. Aims of the Research

1.5.1. General Aims

- To identify that EHR systems need to be dependable, and
- To identify the appropriate risk assessment method applicable to EHR systems

1.5.2. Specific Aims

- To demonstrate that EHR systems are safety related systems**,** and
- To identify the risks associated with EHRs by evaluating the safety, privacy and availability of such systems

1.6. Chapter Summary

This dissertation includes the following chapter structure:

1.6.1. Chapter 1: Introduction

Chapter 1 outlines the structure of the dissertation along with a discussion of the research question, research approach, significance of the research and research aims.

1.6.2. Chapter 2: Electronic Health Record Systems

Chapter 2 reviews the literature of EHR systems. The review starts with definitions of both medical informatics and EHR systems. Various EHR systems from around the world are discussed, including their purposes, functionalities, key capabilities and processes.

1.6.3. Chapter 3: Failures of Computer Systems in healthcare

Chapter 3 reviews the literature related to failures in healthcare systems generally. Different cases of failure are described and analysed in order to glean a better understanding of failures and risks in such systems.

1.6.4. Chapter 4: Dependability of Electronic Health Record Systems

Chapter 4 identifies the relationship between the dependability and data quality of EHRs and the attributes for safety assessment. This chapter reviews the relevant literature in order to develop a theoretical basis of safety. By analyzing dependability and data quality attributes, we deduce the safety attributes of EHRs appropriate for this study.

1.6.5. Chapter 5: Risk assessment of electronic health record systems

Chapter 5 identifies different risk assessment methods, and explains why risk assessment is needed for EHRs. Different risk analysis methods are analysed, and the most appropriate method selected for the risk assessment of EHRs.

1.6.6. Chapter 6: Methodology

Chapter 6 describes the research methodology utilised in this study.

1.6.7. Chapter 7: Case studies

Section 7.1 introduces the case studies. Section 7.2 describes the empirical risk assessment case study in Community Health Information Management Enterprise CHIME, Illawarra. The results of a qualitative case study together with feedback from users are provided in this chapter. Some system improvements have been made as a result of this research.

Section 7.3 describes the risk assessment case study conducted in Maternal and Infant Network **(**MINET) Simpson Centre. This second empirical case study again clearly identifies appropriate safety attributes along with an appropriate method for risk assessment of EHRs.

1.6.7. Chapter 8: Summary and Conclusions

Chapter 8 summarises the research, with particular emphasis on the key findings from the case studies. It also provides recommendations for healthcare organizations, highlights the limitations of this research and suggests directions for future study.

In Summary, Chapter 1 has provided an outline the research undertaken into the risk assessment of electronic health record systems. The next chapter, - Chapter 2 - will explain EHR systems in detail.

CHAPTER TWO

ELECTRONIC HEALTH RECORD SYSTEMS

A thorough understanding of electronic health record systems is important as a precursor to a study on their risk assessment. This chapter therefore incorporates a detailed discussion of EHR systems, including definitions, types, purpose, users and functionality. It should be noted however that not *all* health information systems are EHR systems.

Risk assessment of EHRs is an area of research in medical informatics.

2.1. Medical Informatics Defined:

Medical informatics has been defined as “the theoretical and practical aspects of information processing and communication, based on knowledge and experience derived from processes in medicine and health care” (van Bemmel and Musen 1997).

An alternative definition is “ the field that concerns itself with the cognitive, information processing, and communication tasks of medical practice, education, and research, including the information science and technology to support these tasks” (Greenes and Shortliffe 1990).

EHRs play an important role in medical informatics, as they are involved in the storage, retrieval and use of information for appropriate decision making.

2.2. Health Information Systems

Different health record systems have been used in health care. Automated medical record systems were first developed in the 1960s (Shortliffe and Perreault 1990). The systems most used for processing patients' information are medical record systems, hospital information systems, nursing information systems, laboratory information systems, Pharmacy systems, Radiology systems, Patient monitoring systems, Office systems, Bibliographic retrieval systems, Clinical Decision Support systems, Clinical Research Systems, Medical Education Systems and Health Assessment systems (Shortliffe and Perreault 1990). All these systems can be categorized as health information systems and are used for the purpose of data acquisition, record keeping, communication, integration, surveillance, information storage and retrieval, data analysis, decision support and education (Perreault and Wiederhold 1990).

Health information systems either contain or make direct reference to sensitive health data of individual patients. Thus health data needs to be both secure and free from error. Inaccurate or insecure information could be detrimental to the individual and subsequently to the company or organization responsible. Any computer system where failure could have an impact on a person's health or be life threatening should be regarded as a safety related system. Privacy is now regarded as a pertinent area of growing concern, as more health information is available electronically online (Puplick 2003). Hence, it is essential to develop

health information systems that can be trusted and are dependable. A discussion of dependability and trust is presented in chapter four.

There are many different health information systems currently in use and all such systems need to be dependable. It is beyond the scope of this research to assess the dependability of *all* health information systems. This research will focus on the dependability of EHR systems by exploring safety and risk assessment methods applicable to them.

2.3. Electronic Health Records – EHRs - are the Holy Grail of medical informatics. Clinicians, health systems administrators and policy makers would all benefit from having an electronic record that could capture data along the entire continuum of care (Mandl and Lee 2002). Tange et al. have highlighted the fact that health records should contain clinician's statements, what they have heard, seen, thought and done, and should retain what clinicians believe (Tange et al. 1998).

Electronic Health Records EHR defined -

"Electronic health record assists with clinical matters (reporting results of tests, allowing direct entry of orders by clinicians, facilitating access to transcribed reports, and in some cases supporting telemedicine applications or decision-support functions), but also with administrative and financial topics (tracking of patients within the hospital, managing materials and inventory, supporting personnel functions, managing the payroll, and the like), research (for example, analyzing the outcomes associated with treatments and procedures, performing

quality assurance, supporting clinical trials, and implementing various treatment protocols), scholarly information (for example, accessing digital libraries, supporting bibliographic search, and providing access to drug-information databases), and even office automation (providing access to spreadsheets, word processors, and the like). They are electronic, accessible, confidential, secure, acceptable to clinicians and patients, and integrated with other types of non-patient-specific information" (Shortliffe and Perrault 1990).

"An electronic health record is an electronic longitudinal collection of personal health information, usually based on the individual or family, entered or accepted by health care professionals, which can be distributed over a number of sites or aggregated at a particular source, including a hand-held device. The information is organised primarily to support continuing, efficient and quality health care. The record is under the control of a known party" (NEHRT, 2000).

The U.S. Institute of Medicine defined EHR as "an electronic patient record that resides in a system designed to support users through availability of complete and accurate data, practitioner reminders and alerts, clinical decision support systems, links to bodies of medical knowledge and other aids" (Dick and Steen 1991).

Today, the focus of EHRs is on the integration of 24 hour access by multidisciplinary stakeholders within healthcare systems, removing the concepts of professional boundaries and geographic locations (Wainwright and Warning 2000).

Waegemann (2002) has identified 10 dimensions for EHRs, these being:

1. data content;
2. information capture;
3. information representation;
4. operational dimension and data model;
5. clinical practice;
6. decision support;
7. security;
8. quality assurance;
9. performance, and
10. application

2.3.1. Electronic Patient Records, personal health records and population records

EHRs can also be categorised into Patient records, personal records and population records (Humphreys 2000).

Electronic Patient records are used for clinical care in which doctors, nurses, and other health care professionals within an array of hospital, primary care, other ambulatory and institutional health services.

Personal or consumer oriented health records are for individual use, including assessment of health status and linkage with physician's records.

Population health records are used for health services research for monitoring public health and outcomes. These records used de-identified data from the healthcare system.

However, Waegemann (2002) has identified 5 types of personal health records:

1. Offline personal health records;
2. Web based Commercial/ organisational personal health records;
3. functional or purpose based personal health record;
4. provider based personal health records and
5. partial personal health records.

Kim and Johnson identified personal health records as web-based applications, in which patients can enter their own information (Kim and Johnson 2002).

Offline personal health records are manual health record systems and do not fall within the scope of this study.

2.3.1.1. Personal Health Record in Smart Card

Smart cards or patient-carried medical records were fashionable in the 1980s. However, smart card technology has not gained popularity because of lack of infrastructure (Waegemann 2002) and lack of standards (Dash 2001). Nevertheless, they could become popular again as the technology infrastructure becomes cheaper (Berman 2003; Zalud 2003) or with the potential for immediate access to patient data and reduced duplication of records (Cohen 2003; Berman 2003; Zalud 2003). In Taiwan, a smart card system replaced a paper based health record system in 2001 for the country's 22 million people (Cohen 2003). In Australia, Health Minister Tony Abbot stated that smart card use would enhance

access to an individual's medical record, and that the health system would be in a "systemic paralysis" if a smart card carrying an individual's medical history was not available within five years (Herald Sun news 2003).

2.3.2. The needs for electronic records from a consumer's perspective

Patients often become frustrated because of lack of knowledge of their case by individual health professionals and annoyed at often having to repeat the information several times to different health care professionals (Rigby et al 1998). If EHRs could be shared among different health care organizations, and if the information could be made available at the time of care, it could solve the problem of patients being asked the same information repeatedly from different health care organizations.

2.3.3. EHR Systems around the world

Healthcare institutions started to use EHR systems in the late 60s and early 70s. PROMIS (Problem Oriented Medical Information System) and ARAMIS (The American Rheumatism Association Medical Information System) are two typical systems which started around 1970. With the ARAMIS time oriented medical record system, the search speed for the medical records was four times faster than with traditional paper based records (Tange et al. 1998). The primary purpose of ARAMIS was to serve as a national research data bank for the storage and disclosure of longitudinal data of chronic rheumatologic disease.

PROMIS was developed in 1969 at the Vermont Medical Centre. It included Subjective observation, Objective observations, Assessment and Plan. PROMIS

did not survive because it offered no advantages over paper- based records (van Bemmel and Musen 1997).

During the 1970s and 1980s several computer record systems were used in the medical disciplines, completely integrated with the hospital information system. The Regenstrief system (Indiana University, Indianapolis), was developed to include computer reminders to users of the system and was used at more than 30 clinics (Kuhn and Giuse 2001). Major parts of the medical history, physical examination, and progress notes were not captured in the computer until 1988; complete capture of medical narratives was achieved for obstetrics in 1992(Kuhn and Giuse 2001).

STOR - Summary Time Oriented Record (University of California, San Francisco), HELP (LDS Hospital, Salt Lake City), TMR - The Medical Record (Duke University, Durham), COSTAR (Harvard Medical School, Boston) (Spann 1990; van Bemmel and Musen 1997; Tange et. al 1998), CCC - Center for Clinical Computing, (Beth Israel Hospital, Boston) and DIOGENE (University Hospital, Geneva) are example systems that are still operational and used in various institutions. TMR is the most comprehensive of these systems (van Bemmel and Musen 1997; Tange et. al 1998).

In the Netherlands, an integrated hospital information system was implemented in 1972 in Leiden University Hospital. It has subsequently been expanded into different phases of development, and the system is still in use (Bakkar and Leguit 1999).

Implementation of EHR systems is encouraged in health care institutions around the world. In the United Kingdom, March 2005 is the target for full implementation of first generation person-based EHRs – more specifically all acute care hospitals to implement level 3 electronic patient records (NHS Executive 1998).

Table 2.1. Levels of electronic patient record identified by NHS, UK

Level 1	Patient administration and independent departmental systems
Level 2	Level 1 plus integration via master patient index
Level 3	Level 2 plus electronic clinical orders, results reporting, prescribing, multi professional integrated care pathways

As described previously, EHRs started in the United States in the 1960s. Currently, the Department of Health and Human Services, the American Health Information Management Association, the Department of Veteran Affairs and the Health Insurance Portability and Accountability Act (HIPAA) are emphasizing issues surrounding EHR systems such as privacy, confidentiality and accuracy of healthcare data.

2.3.4. EHR initiatives in Australia

Australian hospitals have been using EHR systems. However the majority have been used for administrative purposes rather than for supporting clinical care (NEHRT 2000). In 1998 the Australian Health Minister established the National

Health Information Management Advisory Council (NHMIC) to advise on the development of an electronic health information system (Australia's health 2002). The Electronic Health Record Task Force was subsequently established in November 1999 to implement a national approach to the EHR. The Task Force has proposed a National Health Information Network to support a system of electronic health records and endorsed a National Health Information Network - HealthConnect in July 2000. HealthConnect is proposed to facilitate the safe collection, storage and exchange of consumer health information between authorised health care providers. HealthConnect identified the following building blocks for eHealth: privacy, consent and access control, standards, event summary identifiers, national architecture and provider directories (Health Connect Program Office 2002). HealthConnect Projects trials were started in the Northern Territory and Tasmania, followed by others in New South Wales and Queensland. Various EHR initiatives and trials are underway in different states - for example, in South Australia, the OACIS clinical information system is in operation across eight public health hospitals (Commonwealth of Australia 2003).

2.3.4.1. New South Wales Health Strategy for EHRs

The New South Wales (NSW) health system has targeted implementation of EHRs by 2010. Patient Administration System (PAS), Point of Care Clinical System (PoCCS), Unique Patient Identifiers (UPI) and the Community Health Information Management Enterprise (CHIME) are essential foundations for the NSW EHR (EHR Working Group 2001).

2.3.5. Purposes of EHRs

Medical records serve the following purposes: to recall observations, to inform others, to instruct students, to gain knowledge, to monitor performance, and to justify interventions (Tang et. al. 2001).

2.3.5.1. The Primary Purpose is to provide a documented record of care by means of communication among clinicians contributing to the patient's care for the benefit of both patient and clinician. It should support present and future care by the same or other clinicians (Schloeffel and Jeselon 2002). Therefore primary uses of EHRs include patient care delivery, patient care management, patient care support processes, financial and other administrative processes and patient self-management (Institute of Medicine 1997).

2.3.5.2. The Secondary Purpose of medical records include medico-legal purposes, quality management, education, research, public and population health, policy development, health service management, billing, finance and reimbursement (Schloeffel and Jeselon 2002; Institute of Medicine 1997).

2.3.6. Primary and secondary users of health data

Physicians, nurses, nursing assistants, therapists and allied health professionals are primary users of health data. Researchers, educators, third party players, business administrators, legal representatives, auditors, employers, public health officials, quality assurors and utilization review staff are all secondary users (Win et. al 2002 a).

2.3.7. Electronic Health Records Functionalities

There are a lot of proven benefits from using EHRs. For example, computer generated alerts increase vaccine coverage (Dini et. al.2001). Sullivan and Mitchell (1995) found that the use of a computer during consultations improves immunization rates by 8-18%, and other preventive tasks by up to 50%. At the Good Samaritan Regional Medical Centre in Arizona, a comprehensive prescribing support system alerted 1,116 times during 13,521 admissions over a six- month period. More specifically it alerted serious risks in 64 out of every 1000 admissions, with 44% of these not being recognized as risk situations by the physician prior to the alert (Sullivan and Mitchell 1995).

Use of integrated EHR systems in consultations can improve clinical performance. Integrated health record systems can assist in decision making through alerts provided from the system, information available from drug databases integrated within the record, and results of laboratory tests available within the system (Bates et. al. 2003).

Properly integrated EHR systems would enhance the sharing of information (Booth 2003), which in turn would increase communication between primary and secondary care healthcare providers. Increased accessibility of EHRs between authorized users would improve timely access to care. Physicians would be better informed about the health status of a patient (Hier et al. 2005), which would definitely improve healthcare decision-making (Hippisley-Cox et al. 2003 p. 1443), and in turn enhance healthcare quality.

2.3.8. Key capabilities of EHR systems

The U.S. Institute of Medicine (2003) has identified the key capabilities of an EHR system. Core functionalities include:

- health information and data,
- results management,
- order entry/management,
- decision support,
- electronic communication and connectivity,
- patient support,
- administrative processes, and
- reporting and population health management

EHRs have different information management services, including (Shiffman et al 1999):

- **Recommendation** services, which determine appropriate activities in specific clinical circumstances;
- **Documentation** services, which involve data collection, storage of observations, assessment and interventions;
- **Registration** services, which integrate demographic and administrative data;
- **Explanation** services, which enhance the credibility of recommendation services by providing supporting evidence;
- **Calculation** services, which measure time intervals, medication dosages and other computational tasks;

- **Communication** services, which include standards for data transfer and data security;
- **Effective presentation** services, which facilitate data visualization; and
- **Aggregation** services, which associate outcome, diagnosis and specific guidelines.

It can be seen that medical or health records are important in information management within healthcare practices. Any wrong data or information could impact on both information management and patient care.

The processes involved in EHR are shown in figure 2.1.

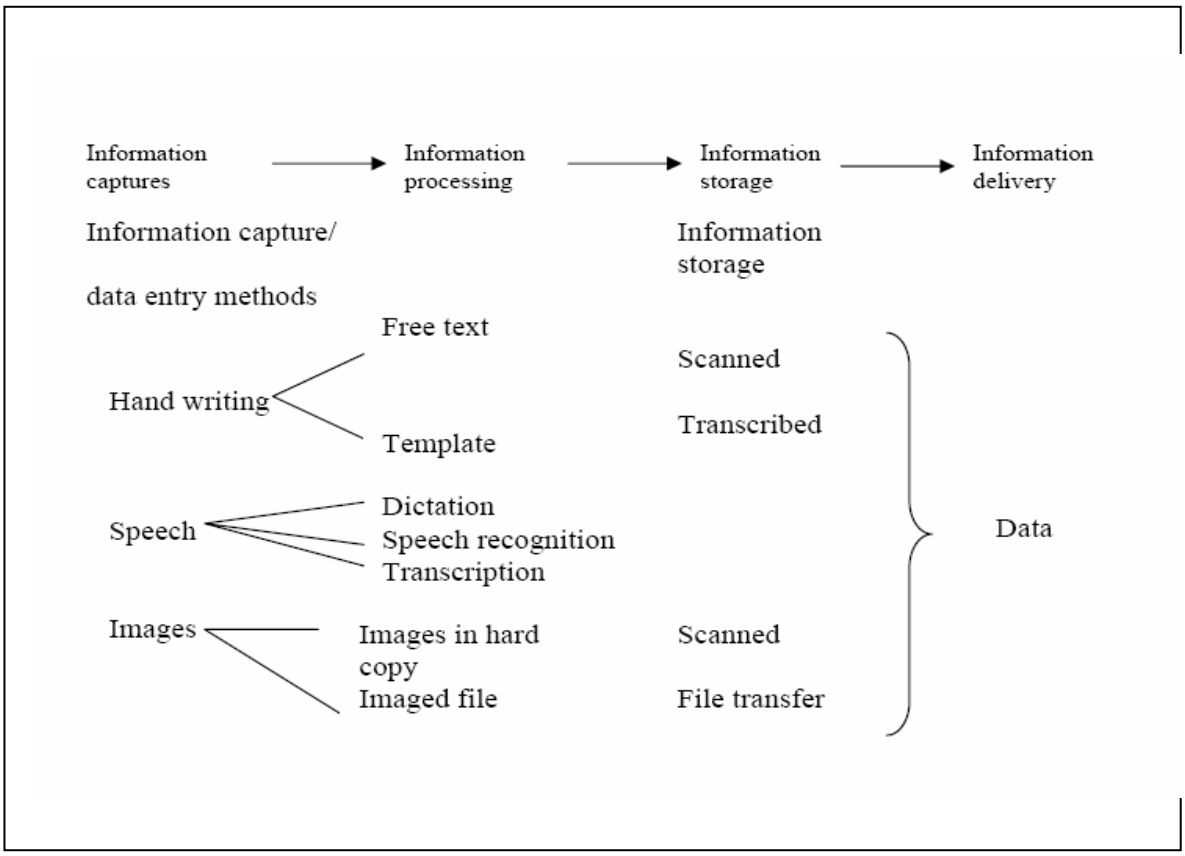

Figure 2.1: Information capture/data entry methods of EHR

2.3.9. Data Entry/ Information captured

Electronic health record systems incorporate both data entry and appropriate retrieval of information for required purposes. Captured information could be from hand writing, speech and/or images.

Hand writing

Information in hand writing can be in free text format, or formatted text in template form. The information can be scanned or transcribed for data entry purposes.

Speech

Data entry can be transcribed through dictation, by way of voice recognition.

Images

Images can be scanned images of Electrocardiograms (ECG), Radiographic images such as chest x-rays, ultrasound images or image files entered from electronic health record systems.

Others

Bar code data entry could be from patient identification wrist or arm band.

2.4. Chapter Summary

Health record systems have evolved from paper-based to electronic systems in healthcare institutions throughout the world, resulting in increased accessibility of information among healthcare providers. Because of this increased accessibility healthcare providers are potentially able to exercise better informed decision-making regarding a patient's health. This is beneficial not only to patients, but also to health care institutions and the healthcare industry generally.

EHR systems include different types of data and information for different users (and for different uses). Information included in health record systems needs to be accurate and health record systems should be safe so that they assist health care workers to improve clinical outcomes.

As described above there are different users of the health records for different purposes and EHR could serve as the effective communication tool between the various healthcare providers.

Accurate information transfer among healthcare organizations would assist the quality and safety of healthcare. Data quality of the health record is vital for accurate information in the health record system.

Integrated EHRs would enhance communication, provide better record keeping and improve communication among healthcare providers. That would be beneficial not only for patients, but also for clinical and research outcomes.

Different EHR systems are in use in different healthcare organizations and it would be difficult to suggest which system is best to adopt for a nationwide or universal EHR. Different health care institutions use different systems according to their needs. There are many schools of thought concerning EHR systems. Some propose that the record's purpose is to support individual patient care, and thus designs which support aggregated data for research, audit, finance or planning are not appropriate (Rector et. al 1991). This would support the basic electronic medical record functionalities, but it would not support *all* functionalities identified by the U.S. Institute of Medicine and other health care organizations.

As described above, EHR systems have different purposes and contain different kinds of data. However it is clear that, appropriate information management of

health records would enhance knowledge management and assist in workflow processes of the organization. These are the positive aspects of the use of EHRs in healthcare. However, there are some resistance to the use of EHRs as analysed below.

As discussed in section 2.3 Mandl and Lee (2002) have pointed out the beneficial effects of EHRs. However, it can be seen that there is a lot of resistance from clinicians to use EHRs. Recent articles in the Washington Post highlighted the preferences of doctors on the use of pen and paper instead of computers (Connolly 2005). There were also cases that computerised order entry system (EHRs) leads to unwanted testing (Holtzman 2004). Therefore, there is a need for user acceptance of using EHRs, and identifying potential errors. By contrast, Hospital administration systems and laboratory information systems have been widely used and accepted by healthcare providers in generally speaking. Hence, there is a need of identifying ways to improve usage of EHRs.

It can be seen that earlier developments of EHRs involved workstations and/or networks of computers, either on Local Area Network or on Intranet. However, one must also realise that these EHRs should assist in the clinicians workflow. It can be seen that healthcare is mobile, - doctors and nurses move around from one bed to another in the hospital ward, ambulatory care healthcare workers make home visits in community care. If EHRs are located only in one fixed place, clinicians need to enter data into a different medium initially then to EHRs later. This increases their workload and errors and inaccuracy can occur. Therefore, EHRs infrastructure also needs to be considered for effective usilisation.

Personal Health Records, - EHRs accessible by patients have been introduced in healthcare to ensure safety. It is envisioned that if patients can access their own

health records, they would be an active partner in their own healthcare, and that will also "demystify those patients who are concerned about what might be hidden in the chart" (Shabo 2004). As discussed in Section 2.3.1. smart cards have been used as personal health records in certain countries; however, there are concerns regarding how much information should be included on the card, dealing with lost or stolen cards, backup and access of records, and so on.

Section 2.3.8 described both the key capabilities of electronic health record systems and the information management services involved in these systems. However, data entry and information capture methods are important areas to be considered for the successful usage of electronic health record systems. As Weir et al. (2003) stated, "Direct text entry of notes (to EHRs) is perhaps the least favourite method of notes generation by providers".

EHR systems around the world and EHR initiatives in Australia are discussed in Sections 2.3.3 and section 2.3.4 respectively. It can be seen that EHRs initiatives and implementations began in the 1960s, however most have been locatd at the University Hospitals or hospitals in collaboration with academic or research institutions, and in U.S. also the Veterans Affairs or Military Hospitals (Ash and Bates 2005). Government initiatives were started around 2000 and Australia has founded the National Electronic Health Record Task Force in 2000 (NEHRT 2000). In U.S. "Got EHR" initiative was launched in early 2005 to promote the usage of EHRs (AMIA 2005). There are a lot of issues regarding successful EHR usage and implementation, and these will be discussed further in following chapters.

CHAPTER THREE

FAILURES OF COMPUTER SYSTEMS IN HEALTH CARE

To be able to carry out risk assessment of EHRs, it is important that risk and failure of healthcare systems are understood. Therefore, this chapter will describe failures of computer systems in healthcare.

Accidents will happen, so it is said; and they do (Redmill 1993).

There is no guarantee that any system is completely safe (Redmill 1993). There is evidence that errors or risks from computer failures cause harm to organizations, their operation or to individuals. Below are some examples from different healthcare industries.

3.1. London Ambulance Service System

The collapse of the London Ambulance Service System is a typical example of safety failure. The service collapsed in October 1992, shortly after the system commenced operation.

3.1.1. System description

The London Ambulance Service (LAS) was designed to accept emergency calls and dispatch ambulances appropriately. The service had coverage of 600 square miles and a resident population of 6.8 million. It was the largest ambulance service in the world. LAS consists of a computer aided dispatch system with automatic vehicle location, which was responsible for tracking available resources, making despatch decisions and locating ambulances.

3.1.2. The failure

The system became overloaded with a large volume of calls and it could not track the locations of various ambulances. Therefore, resource identification, determination and communication did not work properly and there were large numbers of exception messages and duplicated calls, which caused the system to slow down. As dispatches became more delayed, the public began repeating their calls and that further increased the load on the system.

Because of the system failure, emergency medical care was delayed with unnecessary consequences to patients' lives. For example, one ambulance arrived to find the patient dead, one ambulance arrived to a stroke patient after 11 hours, and another arrived 5 hours after the patient had left for the hospital. It was believed that 20 lives were lost as a consequence of the failure of this system.

It was noted that the system could not handle high call volume, as it was not fully tested. There was no reliable back up system and users were not trained properly (Finkelstein 1993, Finkelstein and Dowell 1996, Anderson 1999).

Failure of the London Ambulance System clearly demonstrates that system availability, reliability, system response time and system performance are of critical importance.

3.2. US Cedars Sinai Medical Centre

In the United States, Cedars-Sinai Medical Centre suspended the use of a multimillion- dollar computerised system for doctor's orders in January 2003.

3.2.1. System description

Cedars Sinai Medical Centre invested at least 25 percent of its annual budget on information technology. The Centre identified key performance criteria essential for its Computerised Physician Order Entry System (CPOE) and developed its own comprehensive system in collaboration with Perot Systems. It was piloted and test run for 2 weeks in August 2002 and implemented in October 2002 (Langberg 2003).

However, the system was suspended as more than 400 physicians petitioned stating that it required excessive work and it was endangering patients' safety. Typical such events were (i) patients with heart failure not receiving the relevant pills, and (ii) giving local anaesthetic one day early to a baby for a circumcision (Ornstein 2003).

It was noted that physicians were not familiar with the system, and that changes in workflow impact on patient care.

3.3. Therac 25 (Leveson 1995, Neumann 1995)

Between 1985 and 1987, six patients were massively overdosed because of a computer-controlled radiation therapy machine.

Therac 25 is a medical radiation machine, which accelerates electrons to create high-energy beams that can destroy tumors with minimal impact on the surrounding healthy tissue. Therac 25 was modified from earlier models, Therac6

and Therac20. Some of the Therac6 code and Therac20 subroutines were reused in the Therac 25 development. Therac25 software was responsible for monitoring the machine status, accepting input about the treatment and the setting up of the machine for the treatment. There were altogether 11 Therac25 machines installed; 5 in the United States and 6 in the Canada.

Please see print copy for Table 3.1

Table 3.1: Accidents of Therac25 (Neumann 1995)

Causal factors were overconfidence in software, lack of defensive design, failure to eliminate root causes, unrealistic risk assessment, inadequate investigation or follow up on accident reports, and software reuse without thorough testing in the Therac 25 (Leveson 1995).

Overconfidence in the system caused major consequences to human lives in Therac25. In a different incident, patients complained that there were problems

at the time of the radiation but operators of the Therac25 trusted in the fool-proofedness of the system (Neumann 1989). This illustrates the importance of patient's feedback in patient safety - overlooking this could lead to adverse outcomes. In Therac25, the system did not inform the user that an overdose had occurred which is a serious flaw (Leveson 1995). Error messages could not be understood by the operator and that was a flaw in the human computer interface (Leveson 1995). Users of the system were not involved in system development and they did not know how the machine operated internally. System developers may not have known the potential dangers of the machine, and the system was not tested properly.

3.4. North Staffordshire *under* doses

The North Staffordshire Royal infirmary caused errors in radiation doses for nearly 1000 patients because of a system error. Patients were given less than 10 to 30 percent of prescribed doses over 10 years because of unnecessary adjustment in the computer when it was installed (Neumann 1995). The North Staffordshire Health Authority has paid more than £ 3.1 million to settle legal claims (Blackhurst 2003).

3.5. Chapter Summary

The Cases described in this chapter indicate that accuracy of the system is important. There were problems because of inaccurate doses in both the Therac25 and the North Staffordshire cases.

To prevent failures, the system should be user friendly and easy to use. The Cedars Sinai Medical Centre CPOE failed because the system was not user friendly and also impeded the clinical workflow. There were problems with Therac25 because error messages in the machine could not be understood; the machine was not user friendly. The London Ambulance Service is another case where users were not sufficiently familiar with the system. The system was implemented without being fully tested, it could not handle the load, and there was no back up. The service had a complete system change over which had a major impact on users. System failures can occur when users are not familiar with the system and it does not assist users. Therefore user training is very important for the system to be successful.

Failures from different healthcare systems were discussed in this chapter. There were undesirable consequences from these failures. The Cedar Sinai CPOE case clearly illustrates that health systems should not impede the workflow of healthcare delivery. Therefore, EHRs should be designed to assist healthcare workers in information processing and should not interfere with the healthcare process.

It has been shown that although computers can assist humans, no computer system is immune to failure. There can be unforeseen errors and these could cause loss of trust in systems, loss of human lives, economic losses, and other consequences. Understanding how these failures occurred and analysing these failures could assist in factors to be considered in the risk assessment of different systems. Awareness of the nature, causes and incidence of failures is a vital

component of prevention (Department of Health 2000). As with the adage, "Prevention is better than cure", awareness of failures and minimizing risk could prevent adverse events and losses in the future.

In summary, this chapter has reviewed healthcare computer systems failure. An understanding of these failures will assist in identifying safety attributes for the risk assessment of EHRs.

CHAPTER FOUR

Dependability of Electronic Health Record systems

The dependability of an EHR system needs to be explored to identify safety requirements. By doing so, accidents and failures of the EHR (discussed in Chapter Three, Chapter Five and this chapter) can be minimised to enhance the system safety. EHR systems, their purposes and functionalities were discussed in Chapter Two. This chapter will elaborate on dependability and data quality and propose attributes for EHR systems safety.

It has been established that since EHR systems include patients' health information, it is important that such systems are both trusted and dependable (Win et. al. 2002). The consequence of errors or incomplete information can have minor to significant impact on an individual's life ranging from embarrassment to loss of life. Thus, it is important that these systems are dependable.

4.1. Dependability

Dependability can be explained as follows.

Laprie (1995) and Zviran et al (2003) identified dependable computer systems as needing to have the following attributes:

- Reliability: ensuring continuing service,
- Safety: non-occurrence of catastrophic consequences for the environment,

- Confidentiality: non occurrence of unauthorised disclosure of information,
- Integrity: non occurrence of improper alterations of information, and
- Maintainability: enabling repair and system evolution.

Sommerville (Sommerville 2001), has identified dependability as comprising:

- Availability: the probability that the system will be up and running and able to deliver useful services at any given time,
- Reliability: the probability that the system will correctly deliver services expected by the user,
- Security: a judgement of how likely it is that the system can resist accidental or deliberate intrusion, and
- Safety: a judgement of how likely it is that the system will cause damage to people or its environment

Information security has attributes such as (Andersson 1999):

- Integrity,
- Availability and
- Confidentiality

Pressman has identified availability as an indirect measure of software maintainability (Pressman 2000).

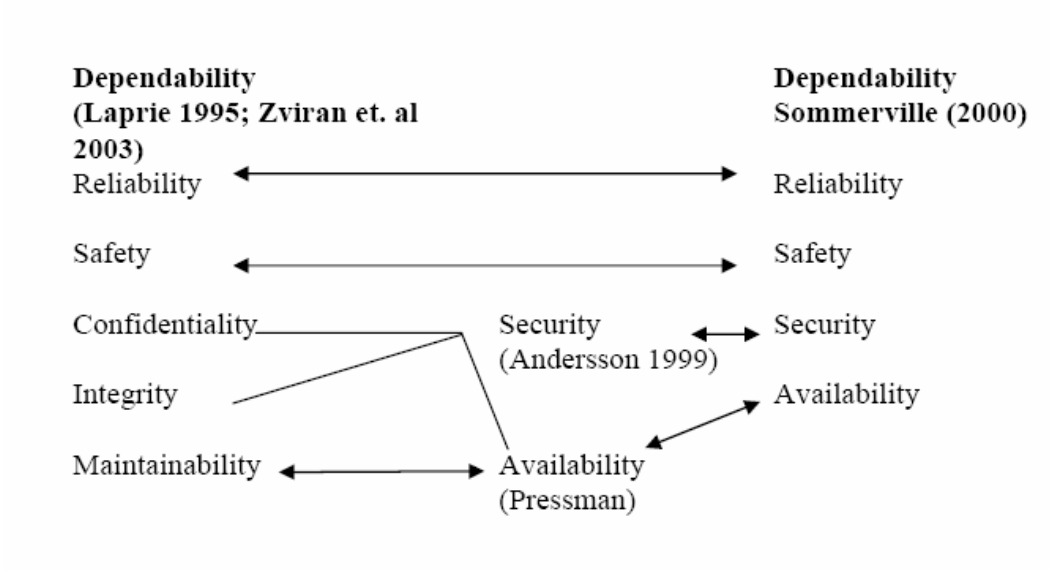

Figure 4.1: Dependability

Accordingly, this research has adopted the dependability categorization of availability, reliability, safety and security (figure 4.1).

In context of EHR Systems, dependability can be subdivided into availability, reliability, safety and security (figure 4.2).

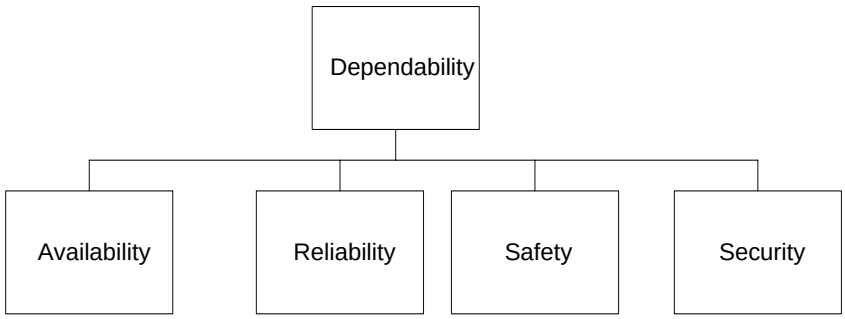

Figure 4.2: Dependability and its attributes

4.1.1. Availability

Availability refers to the total number of hours a system is operational, e.g. non-availability could result in delays in accessing critical health data.

4.1.2. Reliability

This refers to how often a system fails. An unreliable system may at best exhibit poor availability or in some circumstances supply incorrect health data.

4.1.3. Security

This refers to how difficult it is for unauthorised users to gain access to a system and its data. For EHR systems, a secure system will have adequate access control, authentication and encryption measures in place to ensure adequate privacy and to prevent tampering.

4.1. 4. Safety

This refers to the risk that the EHR system can cause harm to an individual.

4.2. Data Quality

Data quality is defined as "the totality of features and characteristics of a data set that bears on its ability to satisfy the needs that result from the intended use of the data"(Arts et al. 2002).

Wherever possible, data quality should not be compromised because low quality health data will have great impact on decision-making processes and tremendous effect on patient management. Data quality is important because appropriate information will assist in the decision making process (Win et. al. 2003 a).

Processing, analysing and interpreting the information could lead to new knowledge and interpretation of this knowledge could lead to decisions (Sauerborn 2000).

Wang and Strong identified data quality as data that are fit to be used by data consumers (Wang and Strong 1996). Health Information Systems consist of aggregated data for diagnosis, treatment, research, finance or planning (Rector et al. 1991), and thus it is important to maintain data quality.

Data quality can be characterized by accessibility, accuracy, consistency, comprehensiveness, currency, definition, granularity, relevancy, precision and timeliness (AHIMA Data Quality Task Force 1998; Moczygemba and Hewitt 2001) (Table 4.1).

Arts et al. have identified accuracy and completeness as the most cited data quality attributes. Based on their literature review, data errors can occur at different steps in the data collection process; data errors from incomplete data entry in medical databases account for 4 percent; inaccurate extraction 1.7 percent; incomplete extraction 1.4 percent; inaccurate data transfer 0.9 percent; 2 percent inaccuracy for automatically collected data; and 6 percent incompleteness in automatically collected data for central registry databases (Arts et al 2002).

The Attributes of data quality are as shown in Table 4.1.

Please see print copy for Table 4.1

Table 4.1: Attributes of data quality (after National Committee on Vital and Health Statistics 2000).

4.3. Data Quality and dependability

Table 4.2 presents characteristics involved in healthcare data quality, how it could be related to the dependability and the appropriate measures needed to ensure the data quality.

Please see print copy for Table 4.2

Table 4.2: Relationship of Data quality and dependability (Win et. al 2002 b)

Data accuracy is important for healthcare because inaccurate data could impact on healthcare decision making and that could cause undesirable effects to patients. The following events are some examples of impact in healthcare from impaired data quality.

4.3.1. Inaccurate information by software

In the United Kingdom, because of the millennium bug error, incorrect Down Syndrome test results were sent to 154 pregnant women. Because of that, four

Down Syndrome babies were born to mothers to whom their tests put them in the low risk group. Two terminations were carried out as a result of mistaken test reports (Wainwright 2001).

4.3.2. Inaccurate information by mistake

A woman in Dusseldorf, Germany was erroneously informed that her test results showed she had incurable syphilis and had passed that on to her daughter and son. As a result, she strangled her fifteen-year-old daughter and attempted to kill her son and herself (Neumann 1995).

4.3.3. Data consistency

In one incident, a lack of data comparison standards resulted in a patient having a severe reaction to a medication. The patient was administered an incorrect dosage because the standard tablet size described in the nursing unit was different from that used by the pharmacy (NCVHS 2000).

4.3.4. Data granularity

There can be a significant difference if the data value is not fully entered or displayed. For example, a patient's temperature of 101.8^{o} F should allow for a decimal point rather than a whole number of 101^{o} F.

4.4. Data entry methods

Data entry can be handwritten into the medical chart and scanned later, either through voice recognition software, pen pad, mouse or touch screen.

4.4.1. Possible errors during data entry

If the data is transcribed or scanned from the handwritten document and if there is illegible handwriting, data entry to the EHR system could be wrong as well. If data is transcribed or scanned later *after* the patient is discharged from hospital or after treatment has been given, erroneous data would have an impact only for the research or next treatment or public health purposes, but if it is *before* the treatment there can be an immediate effect on the health of the patient. For example, if the handwritten data was wrongly interpreted – say from i.v to i.t -. there would be a great difference in giving the dose intra**t**hecally rather than intra**v**enously. In one incident in Denver, there was an infant death because benzathine penicillin for i.m (intra**m**uscular) injection was ordered incorrectly as i.v (intra**v**ascular) (Kaushal and Bates 2002).

Abbreviation should be used cautiously as there can be errors due to misinterpretation of abbreviations. Table 4.3 lists some examples of error-prone abbreviations, symbols and dose designations provided by the Institute for Safety Medication Practices (ISMP 2003).

Please see print copy for Table 4.3

Table 4.3: List of error prone abbreviation (ISMP 2003)

If two medications with similar spellings are displayed next to each other, there can be a substitution error. There can be serious impact on the patient if the wrong medication is administered mistakenly. In one incident, a 31-year-old man died as a result of wrong injection of contrast media intrathecally for spinal radiography. In that incident, the ionic-contrast-media was used instead of the intended non-ionic water soluble radiographic contrast media. The injection was

given intrathecally which is fatal as it can cross the blood brain barrier and cause muscle spasms, convulsions and death (ISMP 2003).

If the drug names are similar and the patient is given the wrong drugs, there may be an adverse effect. The following incidents illustrate the accidental administration of medication with similar names (ISMP April 2003):

> "In a labor and delivery unit, a healthy young woman became hypotensive after epidural anesthesia was administered. A nurse immediately called the obstetrics resident to inform him of the patient's condition. The resident, known to be difficult at times, became angry and snapped at the nurse as he ordered ephedrine 10 mg to be given slow IV push. When processing the order, the nurse, who was anxious because of the physician's behavior, made a mental slip and thought of "epinephrine". With only a few ampoules of epinephrine 1 mg on the unit, she decided to borrow more from the nursery. She found a 30 mL vial of epinephrine 1:1,000 (1 mg/mL), per withdrew 10mL, and returned to administer that amount to the patient. Almost immediately, the patient developed tachycardia, severe hypertension, and pulmonary edema."

Medication dose is important as error in interpretation could have serious consequences to health. In some EHR systems, clinical notes are still entered in plain text format and systems are not integrated with the medication or pharmacy databases. In one incident, a child received an overdose of Phenytoin due to ambiguous use of abbreviations. The patient received approximately three times the indicated dose as the order was misinterpreted. The order was written as mg/kg/d without specifying that 'd' meant day as opposed to dose (Kaushal 2003).

Therefore, there should be a check against possible combination effects for medications, suggested routes of administration for each drug incorporated in the software; and drug potentiation effects from possible combination of drugs.

Data can be keyed into wrong patient records and there could be a possibility of wrong treatment, wrong discharge, wrong operation or missed monitoring, depending on the condition and nature of mixed cases. Therefore for EHR systems, all screens should have the patient's name and identification displayed so that wrong data entry can be prevented.

If gender data is entered wrongly, there can be consequences in reminders such as mammography, pap smears or prostate screening of the patient and there can be wrong scenarios for patient data.

Data verification and validation checks during data entry should be included to improve the reliability of the data. For example, adding algorithms that check against the patient's age and weight can prevent erroneous entry of patient data. If the person's age and weight entered is in unacceptable range, the system will prompt an alert message so that the care provider will know and decide immediately whether it is wrong data entry or whether the patient is in the abnormal weight range.

Doctors are trained to take a history of present illness in narrative styles especially for inpatients, so doctors may prefer to put this in textual format for

present history for the current illness. For that, search facilities can be included to extract the appropriate data to be included in the structured format in the record system. Clinical narratives should be organised within EHR systems to facilitate information retrieval.

EHR systems should not disrupt the workflow of the health care providers. As discussed previously, there is documented evidence of medication errors. Lack of information about the patient and lack of knowledge of drugs strongly influences serious adverse drug events (Kuhn and Giuse 2001). To deter this, many health care institutions started to implement computerized physician order entry systems (Murff and Kannry 2001; Ash et. al. 2002; Payne et. al. 2003). Although these systems are implemented to improve patient safety, some systems failed. An example would be the Cedar-Sinai Medical Centre, Computerised Physician Order Entry System where physicians petitioned to discontinue the system (Discussed in Chapter three). The system was discontinued as there were concerns for safety and also it was disrupting the workflow.

EHR systems should be easily accessible with minimum down time and not involve many complicated steps in data entry.

4.5. Data linkage and integration

As health information systems need to integrate among different healthcare institutions and within the same organization, interoperability, integrity and

comparability of the data should be considered in the integration. Data standards play an important role in integration of different health information systems. Message format standards organizations have developed standards for integration of health information systems. Most message format standards have operated at the level of functional interoperability but not at the semantic level (NCVHS 2000). Therefore message format standards developers and healthcare providers need to corporate in terminology development to harmonise the standards. Data linkage and integration projects have been implemented in different health care institutions around the world.

4.5.1. Possible errors from data integration

Communication with patients and colleagues change as the methods of information exchange change (Coiera 2000). Patients' medical records are shared by different health care institution from different health care providers. Computerized records must be linked from one place to another, to be accessible by different health care providers. Integration of patients' medical records from different institutions is needed for successful sharing of information. To integrate data effectively, patients should be uniquely identified (NSW advisory committee 2000). Unique identifiers would enhance the proper linkage and would assist the rapid and accurate identification of the record (Appavu 1997).

Matching or integration of wrong patient data would have tremendous effect on the person's health, research and public health. If the systems integrated used different units or different systems of measurement, data could be interpreted wrongly when integrated. Different units and measurements such as Kg, lb, mg

and g would make a difference in the treatment and outcome. There can also be different normal ranges for laboratory results from one laboratory to another, which could lead to wrong interpretation of data. Therefore, different data standards could lead to interpreting the data wrongly and that could in turn harm the patient. Hence, a unified data standard is needed for the successful integration.

4.5.2. Interoperability (NCVHS2000)

Interoperability is the ability of one computer to exchange data with another computer.

4.5.2.1. Basic interoperability

Message from one computer to be received by another, but this does not require the receiving computer to interpret the data.

4.5.2.2. Functional interoperability

Messages between different computers can be interpreted at the level of data fields, but neither system understands the meaning of the data in that field. For example, data such as “pain threshold 3”could be read at another computer but the latter may not know its meaning.

4.5.2.3. Semantic interoperability

Semantic interoperability means the information in the field can be interpreted. The level of interoperability between systems should be in semantic operability so that information received could be interpreted the same as the original message. If the interoperability is either basic or functional, there could be mistakes in interpreting the information transfer. Therefore systems need to

follow available data standards. Abbreviations used should be uniform so that they could be interpretable in different systems. For example, PID, interpreted in one system as Pelvic Inflammatory Disease should not be interpreted as the Pulmonary Infectious Disease in another. Like wise BPH - Benign Prostate Hypertrophy - should be interpreted the same in another system, and not as Blood Pressure High; URTI - Upper Respiratory Tract Infection should be interpreted the same and not as Urinary Tract Infection. Patient data monitoring should be the same and should use universal standards such as the APGAR score for newborns so that it can be easily interpretable if it is 7 or 10.

The National Electronic Task Force of Australia has identified two approaches in integrating EHRs, which are part of health information systems. They are a federated system approach and a standard health record architecture approach. Data from different standards are integrated in real time and displayed to the patient and healthcare providers in the federated system approach. In a standard architecture approach, data is aggregated at the information storage level. The New Children's Hospital in Westmead Sydney, NSW has a whole institution EHR federated system available at bed site (NEHRT 2000).

Integration of different legacy systems is important in order to have easy accessibility and improve better decision making, but at the same time it should not impede system speed. The system needs to maintain both search speed and completeness. Different health information systems - laboratory, pharmacy, admission, referral and discharge summary should be integrated. For example,

with the common interface, these systems could be the separated subsystems so that the system would be specific to the specific healthcare providers.

4.6. Unique Patient Identifier

Unique identifiers would allow for the rapid and accurate identification of patients. Unique identification would enable accurate identification and would prevent duplication of records and misidentification, which would enhance efficient patient care. Health care procedures such as invasive testing, blood transfusion and surgical procedures require positive identification of the patient and wrong identification could lead to disastrous outcomes. The following scenarios demonstrate why unique patient identification is important for healthcare (Chassin and Becher 2002).

> "Joan Morris (a pseudonym) is a 67-year-old woman admitted to a teaching hospital for cerebral angiography. The day after that procedure, she mistakenly underwent an invasive cardiac electrophysiology study.
>
> The patient, a native English speaker and high school graduate whose daughter is a physician, had been well until several months earlier, when she fell and struck her head. Magnetic resonance imaging showed two large cerebral aneurysms. The interventional radiology service admitted her for cerebral angiography.
>
> The day after admission, cerebral angiography was performed, and one of the aneurysms was successfully embolized. The second aneurysm was deemed more amenable to surgical therapy, for which a subsequent admission was planned. After angiography, the patient was transferred to the oncology floor rather than returning to her original bed on the telemetry unit. Discharge was planned for the following day. The next morning, however, the patient was taken for an invasive cardiac electrophysiology study.

> Approximately 1 hour into the procedure, it became apparent that Ms. Morris was the wrong patient. The study was aborted, and she was returned to her room in stable condition" (Chassin and Becher 2002).

Unique patient identification is important as patients' healthcare processes need to be linked from one episode to another. Correct identification of patient is clearly important for the process of patient care.

The need for a unique patient identifier for electronic health record system has been discussed in many countries. In 1994 the American Medical Informatics Association Board of Directors initiated a discussion on standards for medical identifiers, codes and messages for integrated computer based health records (Board of Directors AMIA 1994). An American National Standard, Standard guide for a Universal Health Identifier has identified criteria and characteristics of a Universal Healthcare Identifier (UHID) and specified that they should meet at least the criteria listed on table 4.4. (E1714-00).

Accessible	Disidentifiable	Mergeable	Splittable
Assignable	focused	Networked	Standard
Atomic	governed	Permanent	Unambiguous
Concise	Identifiable	Public	Unique
Content-Free	Incremental	Repository based	Universal
Controllable	Linkable	Retirement	Usable
Cost-effective	longevity	Retroactive	verifiable
deployable	mappable	Secure	

Table 4. 4: Criteria and characteristic of universal health care identifier

It can be seen that there are different criteria to be met. Currently, public hospitals in Australia use Medical Record Number (MRN), or Patient Master Index (PMI). However, there are different identifiers in private hospitals and general practice. The NSW Health Council recommended a state-wide UPI in 2000. One of the limitations of the current health system, identified by the NSW Health Council in 2000 was the lack of a *single* identifier to allow health providers to identify with certainty the identity of the particular individual they are providing services to (Cornwall 2000). Therefore, unique identification of patient is essential for safety of the EHRs.

4.7. Data standards

Methods, protocols, terminologies and specifications for the collection, exchange, storage and retrieval of information associated with healthcare applications can be regarded as healthcare data standards. A lack of uniform data standards can result in error and could have serious consequences to a patient's life. In one incident, a patient died because information about their allergy to a particular anesthetic was not presented in a standard format and was overlooked when the patient was prepared for surgery (NCVHS2000). There are issues regarding differences in meaning intended by the data entry and individual retrieving for data analysis. Data from EHRs will be used as historical data or aggregated data for analytical purposes. Thus imprecision or lack of standards can create problems. In the example that Shortliffe and Barnett (2001) give, one physician noted that a patient had "shortness of breath"; another physician noted the same condition as "dyspnea". Although these words have the same meaning,

it can be missed in some automatic flowcharting programs or decision support systems, if synonyms are not included. Therefore data entry needs to follow the standards and coding systems.

The following section includes the standards from different organizational body related to health sectors.

4.7.1. Australian Standards

AS/NZS 4804 Occupational Health and Safety Management System

AS 2828-1999 standard for Paper-based health care records, Australian Standard From Standard Australia.

HB 228:2001 Guidelines for Managing Risk in Healthcare Sector (HB-228-2001)

AS ISO 15489-2002 Australian Standard: Record Management highlights the record management requirements, designing and implementing record systems, record management process and controls (AS ISO 15489).

AS 4937-2002 Electronic messages for exchange of claim and related information was prepared by Committee IT – 014, Health Informatics and published on 2 May 2002 (AS 4937- 2002). This standard is related to health insurance claims.

The Draft Health care Client Identification Standard is looking into data capture, guidance on messaging, data matching, privacy and security (HIMAA 2001).

4.6.2. Health Information Standards

Beale 2001 has pointed out standards in health informatics tend to be judged in terms of themselves, against particular local requirements or against each other

(Beale 2001). Health Information Standards present are models approved by authority and specify hardware or software, communication protocols or data definitions and are organized in four general categories: vocabulary, structure and context, messaging and security (Murphy and Brandt 2000).

ASTM (The American Society for Testing and Materials) has developed standards related to electronic health information, these being:

E1384-01 Standard Guide for Content and Structure of the Electronic Health Record;

E1714 Guide for the properties of electronic health records and record systems;

E1762 Guide for electronic authentication of health information;

E1769 Guide for the properties of electronic health record and record systems (http://www.astm.org).

4.6.3. HL7 is the standard for the exchange, management and integration of data that supports clinical patient care and the management, delivery and evaluation of healthcare services (Bakken et al. 2000, Huff 1998)

4.6.4. DICOM Digital Imaging and Communication in Medicine (www.dicom.org)

4.6.5. NCPDP data interchange and processing standards to the pharmacy service sector of the health care industry (Murphy and Brandt 2000)

4.6.6. Safety Standards

There are safety standards to measure and define the acceptable behaviour of processes in the disciplines involved.

IEC 61508 is the standard of safety for all electrotechnical computer based systems (IEC 61508). It is not a system development standard, rather it is the standard for management of safety through the entire life of a system from conception to decommissioning.

MOD 00-55, Requirements for safety related software in defence equipment,

MOD 00-56 Safety Management requirements for defence Systems,

MOD 65 Defence Stan Series – Medical,

IEC 60601 Safety Standard for Medical Electrical Equipment,

As described above, there are standards for safety systems, electronic medical requirements, paper based records, record management standards, messaging standards from different international standard agencies and Standards Australia. However, safety standards for electronic health records are not yet identified in these standards and the researcher has identified this in early 2002 and submitted a paper titled, “Setting a safety standard for electronic medical records”, to HIC2004 Conference and presented regarding this. After this presentation, authors (the researcher and supervisors) have been contacted to give permission to release the paper and the paper was quoted in preparation for National Health Information Standards framework 2003-2007.

4.8. System Security

Information security of a health information system is important as it is in any information system. Health data contains sensitive information of a person's health and it could affect their life. Security of EHR systems could be implemented by the physical security of the system, providing authorised access to the user, firewall and encryption technologies. Security included in the Alberta Computer Record Systems where users need to punch in a unique identification number along with an electronic tag with constantly changing digital number (Cotter 2003) is one example of how security can be implemented.

Sensitive health information such as HIV status, obstetrics history and mental history would be easily accessible, when health records are fully automated. If sensitive health information is accessible by others, it would be a breach of the patient's privacy. It is essential to ensure that health information is disclosed only with the patients' consent except in emergency situations or if it is important for public health purposes.

Confidentiality, integrity and availability are attributes of information security (described in section 4.1) (Andersson 1999).

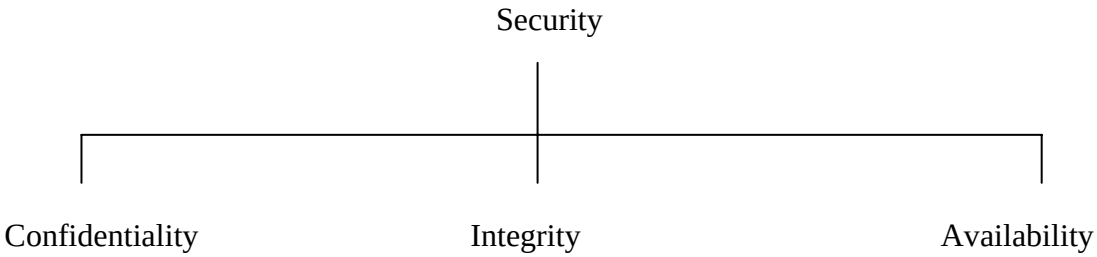

Figure 4.3: Security and its attributes

Integrity is the prevention of unauthorized *modification* of information.

Availability is the prevention of unauthorised *withholding* of information.

Confidentiality is the prevention of unauthorized *disclosure* of information.

Confidentiality is a form of informational privacy characterised by a special relationship such as physician-patient. Personal information obtained in the course of that relationship should not be revealed to others unless the patient is made aware and consents to disclosure (Gostin et. al 1993).

Since the fourth century B.C. and according to the Hippocratic Oath, doctors have needed to maintain patient confidentiality (Medical Record Privacy 1999, AHIMA 1998).

> "Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret" (The Oath by Hippocrates, 4th Century, B.C.E.).

4.8.1. Privacy and Confidentiality

As EHRs become more computerised and integrated among different healthcare providers, data can be accessible from different places by different users and invasion of privacy becomes a higher risk. To maintain privacy and confidentiality, a system needs to be secure. Security is one of the attributes of dependability. Issues of confidentiality and abuse of data cause many health care providers to oppose the coordination of medical databases despite the potential benefits (Gaithersburg 2000). Therefore, implemented EHRs need to ensure privacy and confidentiality.

Healthcare providers and other stakeholders have a duty to maintain the confidentiality of data and systems, and need to deter access by unauthorized users. Users should abide by the law of privacy. Furthermore, legislation should be enacted in line with the changing technology. Advancement of technology increases user accessibility and privacy protections involve use of technology. Healthcare providers' reluctance to share information in local area networks can be overcome by providing adequate technology to support security measures and privacy legislation to produce health data (Amatayakul 1998). Protection of patient records can be achieved by implementing security policies to control access, appropriate authorization before releasing the health data and providing additional security measures to more sensitive data (American Academy of Paediatrics 1999).

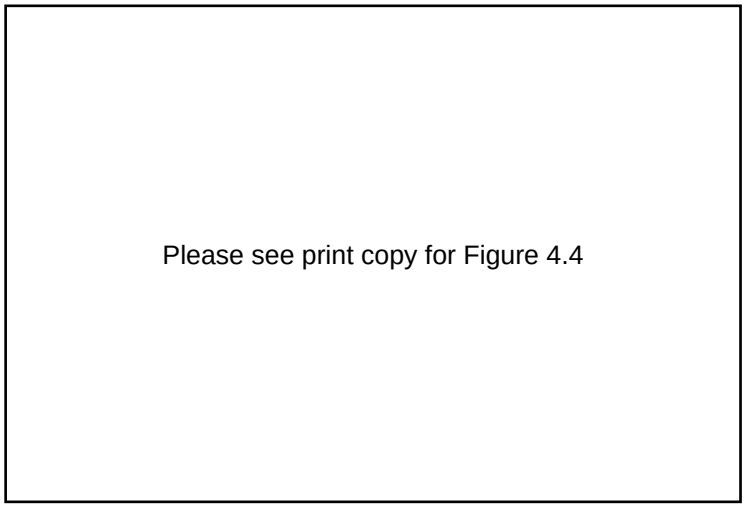

Figure 4.4: Venn diagram: User, Technology, Legislation (Win et. al. 2002a)

4.8.2. Consent, disclosure

Disclosure is the revealing of identifiable health information to anyone other than the subject (BMA ethics 2001).

Healthcare providers need to disclose confidential information where a failure to do so would constitute a threat to public or private interests - for example: reporting communicable diseases to the appropriate health organization. However, if the patient is to be identified, it is important to have the patient's consent for use of this health information. For example, in New Zealand in 1983, a general practitioner was charged because he had disclosed the patient's heart condition, which can be dangerous for driving children's school buses, and the patient sued him in court (Gerber 1999). Although cases could be dealt with differently in different countries, it is advisable that the need to disclose sensitive information to the governing authority should be discussed with the patient and the patient's permission sought, - that is getting consent, -before hand.

Consent means a patient is informed and gives voluntary agreement to confide or permit access to or the collection of information. Consent in medicine, in both the context of therapy and research has been debated since the Second World War -, that is the need for informed consent and the necessary flexibility of its applications (Dalla-Vorgia et al 2001).

Implied consent is where agreement may reasonably be inferred from the action or inaction of the individual and there is good reason to believe that the patient has knowledge relevant to this agreement (Draft Health Privacy guidelines 2001).

Express consent is the consent given explicitly, either orally or in writing. Express consent is equivocal and does not require any influence on the part of provider seeking consent (Draft Health Privacy guidelines 2001).

Many organisations with access to health information have not obtained the individual's consent for disclosing personal information (Gaithersburg 2000). Effective notification and truly informed consent requires that individuals know and understand the contents of the record. It is unethical to use implied consent when the patient is not fully aware of the information disclosure.

The UK Data protection act of 1998 covers sensitive data, defined as health data which cannot be processed in the absence of explicit consent unless they are needed for medical purposes or undertaken by a professional who in the circumstances owes a duty of confidentiality. (Data Protection Act 1998)

There is increasing emphasis on patient autonomy and patient's rights. Patients need to know how the information will be kept, who can access their records and for what purpose. (Waegemann 2000) Patients' medical data can be revealed only with the patients' consent except in emergencies or when the law obliges the healthcare provider to do so (American Health Information Management Association 2001). In certain serious medical situations, the doctrine of implied consent allows it to be assumed that a patient would provide consent if the patient were competent, even though the patient is incapable of communicating consent, unless the patient has explicitly stated refusals to allow emergency release (Rind et. al 1997).

The issue of ownerships of medical records has a large impact on the privacy and access of patient information. (Mandl et. al 2000) Many hospitals consider they own data in the medical record systems and patients consider that their medical information is their own (Schonberg and Safran 2000). Health records consist of objective factual material and the subjective opinions of the treating doctors. (House of Representatives Standing Committee on Legal an Constitutional Affairs 2000). Therefore the doctors copyright interest should be respected and should that override the patient to access his or her health information? The question is debatable and there is a difference of opinion as to who owns the record, - even legal opinion is divided. The supreme court of Canada (1992) maintained that the right to information in the medical record has personal right to the patient, although the file remained the property of the hospital (Knoppers 2000). Personal health record (PHR) systems implemented in U.S and Europe

demonstrate that consumers/patients have rights to access their records. PHR allows consumers an opportunity to create and maintain their own health records (Win and Selakovich 2004). If these PHR systems are to be integrated with the EHRs then patients could grant permission to different healthcare providers to access their records.

To protect patient privacy, integrated EHRs must be access- controlled. As EHRs would be integrated between healthcare organisations, access levels become important for the system. There can be role based access mechanism among the healthcare providers within the organization such as doctors, nurses, and administrative staff. Each clinical record must be marked with a list of accessible names.

The following example will illustrate why access levels of different individuals within the organization is important.

> “A West Coast psychotherapist is finishing up work at the end of a long day when she gets a call from a clerk in the "quality assurance" division. The clerk is processing some of the electronic paperwork generated by one of the psychotherapist's patients and just needs a few clarifications in order to put the forms through.
>
> "I see that you've coded this guy's diagnosis as DSM-IIIR 300.02 Generalized Anxiety Disorder," says the clerk, referring to one of the diagnostic codes in the Diagnostic and Statistical Manual of Mental Disorders, Third Edition (revised).

"Yes, that's right," answers the psychotherapist.

"The plan won't accept that one. You need a more specific diagnosis" says the clerk. "Well I was wondering... I see here that this guy was sexually abused as a kid, so how about if we change this to a 309.81, 'Post-traumatic Stress Disorder'. We use that one a lot here."

The psychotherapist is taken aback. Apparently the full text of her therapy notes, filed with the patient's electronic medical record, is available to the health plan's clerks, accountants and insurance adjusters (Stein 1997).

The example clearly demonstrates that there should be different access levels within the organization according to the user and the purpose of use. As patients are consumers of the system and the information in the health record is information related to them, it is important to maintain the confidentiality level according to patients' wishes. Therefore, the level of access to various systems of the record can be controlled by the level of consent given by the patient. There could be opt-in and opt-out models for such a consent mechanism. Coiera and Clarke (2003) identified the following consent models - General Consent with Specific Denials and General denial with specific Consent (Coiera and Clarke 2003).

General Consent with Specific Denials

In General Consent with Specific Denials, a patient attaches specific exclusion conditions to their general approval to the record for future accesses (Coiera and Clarke 2003).

General Denial with Specific Consent

In a General Denial with Specific Consent model, a patient issues a blanket block on all future accesses, but allows the inclusion of future use under specified conditions (Coiera and Clarke 2003).

General Denial with the Specific Consent has maximum privacy as patient's consent is required for any single access and it may not be suitable to integrate into the electronic health record systems as it may impede the workflow of health care providers, particularly in emergency situations. System administrators may be able to override the consent mechanisms. However, if consent is treated as a legal document and healthcare providers' access the record without the permission, there can be serious consequences and there should be legislation for that situation.

There can also be negative consequences if the patient condition is not known due to access denial. The example would be a patient with heart murmurs due to Aortic incompetence, where it is due to tertiary syphilis, but if the patient's sexually transmitted disease information is not available, diagnosis of the underlying condition could be missed.

There could also be a risk to healthcare providers if a patient's violent behaviour is not known due to the consent mechanism. Therefore, there is a balance between the denial and access of consent mechanisms. Consent is important for the consumer trust and respect the patient autonomy. Consent mechanism that

gives the patient control over the records should not undermine the healthcare delivery process (Win et.al 2003 b). There should be overriding mechanism for monitoring or reporting for the interest of public health. Although the focus of healthcare has changed from Healthcare Providers' paternalistic approach to consumer consent- based approach (Win et al 2002 c), implementing consent should not impact on the healthcare and treatment.

4.8.3. Threats to Confidentiality

Threats to confidentiality of medical records can be from insiders: innocent mistakes such as accidental disclosure, abuse of their record access privileges (Garfinkel 2000). The University of Michigan Medical Center patient records were left exposed to the public on the Internet because they thought that they were on a special server protected with a special password (Carter 2000). It was an innocent mistake but patient's confidentiality was breached. The case of the Florida state public health worker who brought home a computer disk with the names of 4000 HIV positive patients and sent the names to two Florida newspapers (Stein 1997; Jurgens 2001) was a case of abuse of access privilege and access for spite of profit.

Medical records can be the target of unscrupulous attackers. Linked EHRs with unique identifiers can be more easily accessed for quality care. It can also be argued that they are more vulnerable to security breaches because that will also lead to increase accessibility to the unauthorized person. Passwords and other technologies such as encryption, public key infrastructure, firewalls and other

network service management tools together with the patient consent mechanism, could provide more security for EHR systems.

4.8.4. Privacy and Medical Research

There is a need to balance the public interest in medical research against the public interest in privacy. (Guidelines under Section 95 of Privacy Act 1988) Medical research should be carried out in such a way as to minimize the intrusion on people's privacy; consent must be obtained or de-identified information should be used.

The British Medical Association has stated use of information for research is currently accepted as long as it is carried out within the guidelines and subject to monitoring by appropriately constituted research ethics committees, but patients should know that it may involve use of their records (BMA ethics 2001).

Researchers worry that requirements for patient's consent and anonymitization will undermine their research (Evans and Ramay 2001; Roberts and Wilson 2001;Cox 2001). Production of substandard flawed research is less ethical than the use of anonymised data by professional researchers (Roberts and Wilson 2001). If need to maintain surveillance is overridden by patient's privacy, effective monitoring of vaccines safety, outbreak responses, control of infectious diseases can be undermined (Evans and Ramay 2001). Because of the need of patients consent universal inclusion of data is not possible. For example, cancer registry in Germany failed to achieve its mission as the informed consent is required according to the law (Dudeck 2001). Data gathered from the

multicenter acute renal disease registry was limited use because only 52 percent of subjects provided informed consent (Ingelfinger and Drazen 2004).

Patients' confidentiality should not be compromised by selling or providing patients' records. (Dearne 2001) Iceland has sold the medical and genealogy records of its 275,000 citizens to a private medical research company (Reykjavik 2000). Is it ethical for the government to sell the citizens' medical data for the research purpose? Can it be sure that the data will be used only for beneficial effects? Can the government interest override the public interest? It is justifiable for the Iceland government as the Iceland Parliament adopted the Act on health sector databases in 1998 December stating that data entered in the health sector databases are the property of the Icelandic Nation (Knoppers 2000).

In 2001, news broke that Health Communication Network (HCN), a privately owned Australian e-health company planned to sell the information gathered by its software (Murray 2001). Although HCN has stated the patients record will be de-identified, it cannot be guaranteed that it is *not* identifiable. (Murray 2001) This news has alarmed the privacy concerns of the public. It is a misuse of data by a third party because HCN software has gathered the data *without* the full knowledge of the GPs using their software. This incident points out that health care providers need to have knowledge of technology so that unethical use of data can be prevented.

4.9. Safety

Data safety is important as data safety, software safety and system safety are all related. Data safety is concerned with correctly accessing the data and ensuring that there are no errors in it.

For the delivery of safer, higher quality care, systems of care need to be redesigned. This includes the use of IT to support clinical and administrative purposes (Institute of Medicine 2001).

After the release of a report 'To Err is Human: Building a Safer Health System (Kohn et al. 2000), the importance of safety has been emphasised in health care. It was reported that 98,000 Americans die each year as a result of preventable medical errors. The U.S. Institute of Medicine estimates the numbers of lives lost to preventable medication errors alone represents over 7000 deaths annually, which is more than the number of injuries in the workplace (IOM 2000). A national survey from New Zealand has documented that 4.5 percent of all admissions were associated with highly preventable adverse events (Davis et al. 2001). In Australia, it has been estimated that more than 55,000 patients become disabled and as many as 18,000 unnecessary deaths occur each year due to medical errors (Weingart et al. 2000).

4.9.1. Error

Error is a failure of a planned action to be completed as intended or use of a wrong plan to achieve an aim (IOM 2000). Failure and errors can be identified

as human, organizational and technical (Battles an Lilford 2003). Failures can be categorized as active or latent.

Active failures are errors and violations committed by those in direct contact with the human-system interface. They are the unsafe acts committed by people who are in direct contact with the patient or system (Reason 2000).

Latent failures are hazards resulting from the delayed consequences of technical and organizational actions and decisions (Battles and Lilford 2003).

The Swiss Cheese Model represents how active failures and latent conditions could cause medical errors. However, there are different opinions regarding the Swiss Cheese Model of medical errors. Vindal has stated that medical errors are not caused by big holes in the model resembling Swiss cheese (Vindal 2003). He argued that medical errors are not created by big holes in the system. Rather, they are created by simple systemic failures (Vindal 2003). Wong stated that medical errors are not a single event associated with multiple factors and could be represented by the Swiss Cheese Model (Wong 2002).

Bates et. al have identified that high complexity is a risk factor in clinical medicine and that information systems have the potential to prevent adverse events (Bates et. al. 1994).

4.9.2. Errors in medication

Possible errors from different causes of medication is listed in Table 4.5. It can be seen that correct patient identification, correct medicine, dose, route of administration and frequency of dosages are important. It is advisable to integrate

the pharmacy system with drug dosage and calculation so that accidental wrong calculation of doses can be prevented.

Please see print copy for Table 4.5

Table 4.5: Medication errors (Shojania 2003)

The following example shows dosage miscalculation for the medication that could be prevented by including a calculation function for medication in the health record system (ISMP 2003 (2)).

"A physician ordered a heparin infusion with directions to follow a weight-based nomogram for laboratory monitoring and dose adjustments. Later that evening, the nomogram indicated that a bolus dose of heparin 1,700 units IV should be administered based on the patient's a PTT level. The patient's nurse removed a 10 mL vial of heparin (1,000 units/mL) from an automated dispensing cabinet to prepare the dose. However, she miscalculated the volume that was needed as 17 mL, not1.7 mL. The nurse, concerned that she would be using a second vial of heparin to prepare the bolus, quickly asked another nurse to "look at my math" to make sure she had not made an error. But the other nurse did not actually recalculate the volume needed, so she made the same error when "looking over" her colleague's work. The patient received 17,000 units of heparin. A physician's assistant discovered the error after the patient developed severe epistaxis" (ISMP 2003 (2)).

Please see print copy for Table 4.6

Table 4.6: Medication prescribing errors in a teaching hospital (Lesar et. al.1990).

Please see print copy for Table 4.7

Table 4. 7: Medication errors in the HIV-infected population (Purdy 2000)

Table 4.6 illustrates different types of medication error in a teaching hospital. Purdy (2000) has identified medication errors from the HIV infected population, and these are summarised in table 4.7.

4.10. Mapping adverse medical events

Adverse medical events can be mapped into medical cause, IT effect, IT cause and non IT cause.

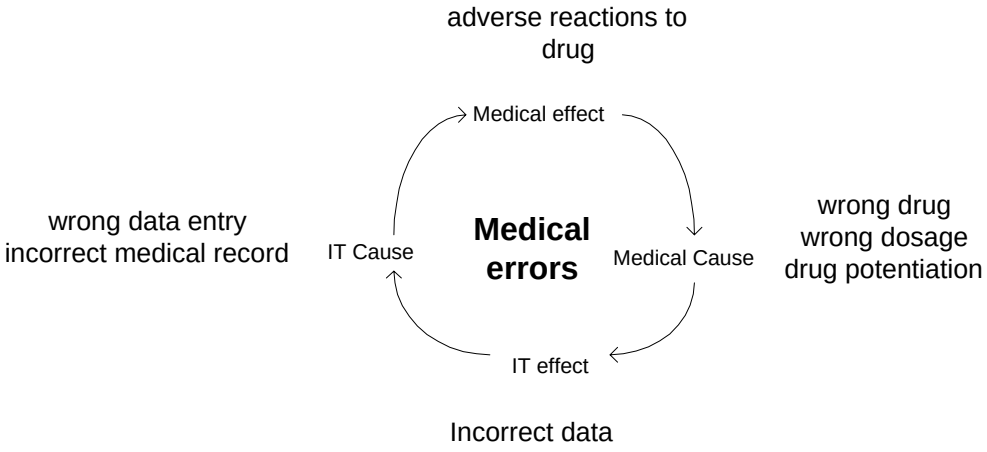

Figure 4.5: Directive graph of medical errors

As described in figure 4.5 errors can occurr in any stage, Causes and effects are interrelated, and can be illustrated by way of a directive graph. The adverse effects of medical errors can be more comprehensively analysed by risk assessment methods.

As in all systems, errors can be due to human error, the underlying system or the nature of the application. EHRs may not harm *directly* but it may occur as part of an overall system. Therefore, to detect errors from EHRs, the patient care processes and work situation related to EHRs should be analysed. Depending on the EHR of interest (Chapter 2), the processes in different EHRs may vary for diagnostic processes, treatment processes, research purposes, preventive care purposes and so on.

Errors can be from different causes and can lead to an accident. Heinrich's Domino theory (Cox and Cox 1996) identified that injuries are caused by the action of preceding factors and removal of the events leading up to the accident would prevent accidents and injuries. Therefore, removing or preventing the unsafe condition can prevent the accident.

4.11. Reliability

EHRs need to be reliable and information retrieved by the system must be correct. Failures due to power outages, system failures and hardware failures should be as low as possible. There should be backup and disaster recovery plans for the system.

4.12. Cause and effect relationship of impaired quality data

Cause	Effect
▪ Inaccurate information by software ▪ Data not accessible due to destruction of data ▪ Data not accessible due to malfunction in hardware or software ▪ Incomplete data due to incomplete transfer ▪ System not functioning properly ▪ Mismatched records ▪ Missing results	▪ Wrong diagnosis ▪ Wrong medication ▪ Wrong dosage administration ▪ Unnecessary repetition of laboratory test ▪ Miss diagnosis ▪ Poor public health information ▪ Unnecessary spending of healthcare dollar ▪ Late diagnosis ▪ Late timely treatment

Table 4.8: Examples of Cause and Effect

Impaired data quality can result from a fault in the system. Therefore, data entry, data capture, data storage, integration of data, communication, data retrieval and

data security all play an important role in the data quality for health information system. As stated previously, impaired data quality can have a direct impact on patient's health. Table 4.8 outlines some of the cause and effect of impaired data.

Wigertz (2001) has stated that successful computer-based patient records are rare especially outside primary care, because of lack of user involvement in the development phase and the resulting low acceptance by user groups of clinical physicians, nurses and paramedics. Therefore, user involvement is important in system development and not only the data quality but also the system quality such as usability, accessibility and ease of use are important, as these could indirectly affect the patient care.

All the effects listed in table 4.8. can be caused by errors in data. Therefore to reduce error and to ensure safer EHR systems, data quality, dependability and all the processes involved should be considered. Figure 4.6 shows the relationship framework for dependability and data quality of the EHR systems proposed for this study. Based on the literature review and this framework, checklist for the safety of the electronic health record systems could be developed.

For EHR systems, non-availability could result in data inaccessibility. Reliability qualifies the frequency of failures, and safety considers the failure and consequences of failure (Thane 1997). Data availability to authorised users is important in order to prevent errors. Therefore safety assessment of the electronic health record systems will ensure system dependability.

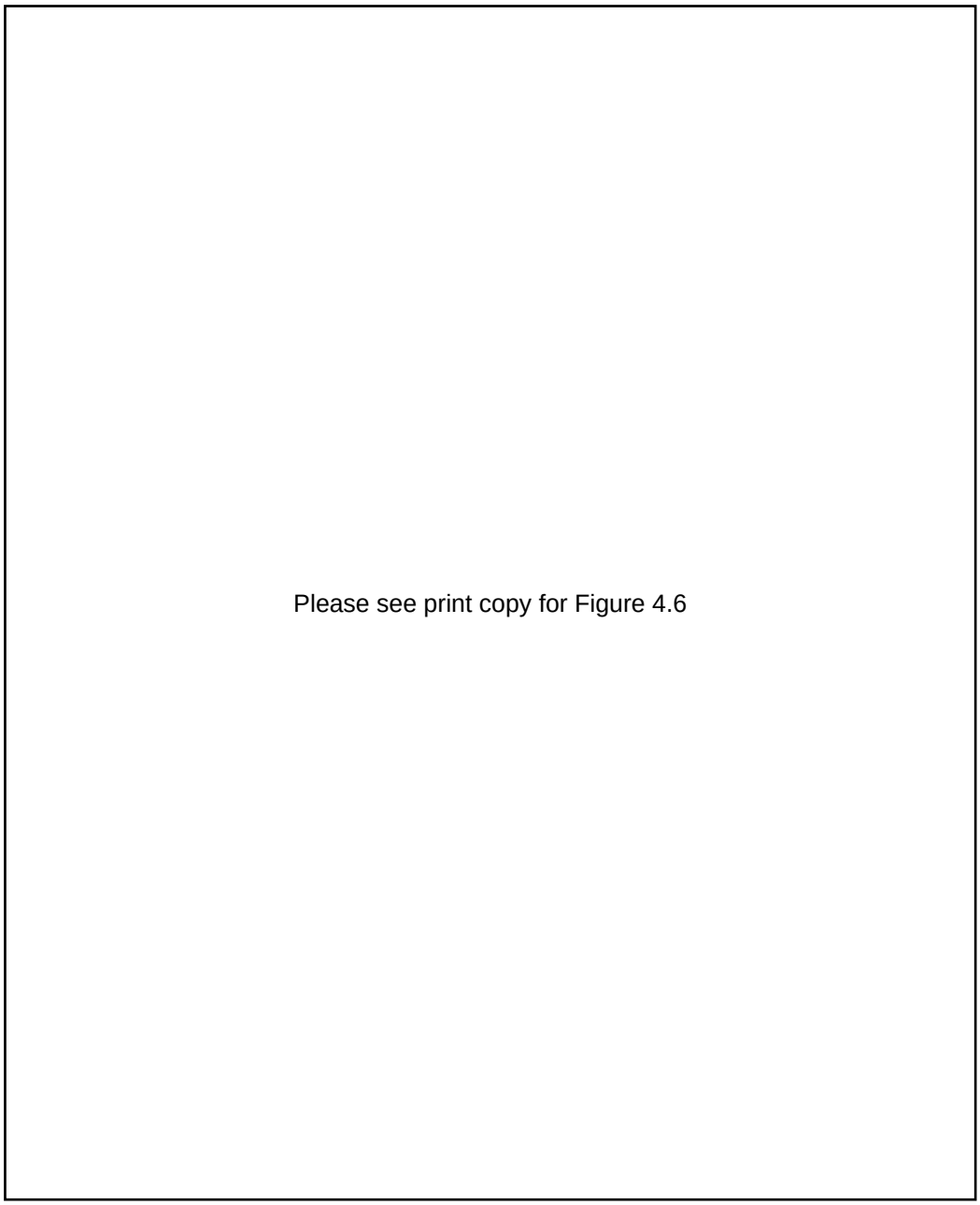

Figure 4.6: Data and Decision-making (Win and Croll 2005)

As shown in Figure 4.6, inappropriate data, table 4.2 can occur in any step involved in information processing; data entry, data collection, data processing and data transmission. Therefore, the appropriate safety attributes for EHR systems are summarized in table 4.9.

- Identification
    1. Unique patient identification
    2. Patient's name and identification on every screen
- System security
    1. Local area network/Internet
    2. Encryption
    3. Authorization
    4. Firewall
    5. Access level
    6. Access list
    7. Antivirus
    8. Audit trail data
- Privacy
- Confidentiality
- Consent
- Disaster recovery
- Storage
- Back up
- Retention period
- Data standards
- Data interoperability
- Data integrity
- Medication
    1. Drug allergy
    2. Drug potentiation
    3. Calculation of dosage
- Alerts
    1. Allergy
    2. Drug potentiation
- Data entry
    1. Data verification
    2. Data validation
    3. Algorithm such as age and weight check
- Attributes of data quality
    1. Availability
    2. Accuracy
    3. Completeness
- System Quality

1. Usability
2. Accessibility
3. Ease of use

Table 4.9: Safety attributes of electronic health record systems

As discussed in Chapter 2, there are different types of EHR systems and any safety assessment needs to accommodate this.

4.13. Chapter summary

Data quality, dependability and safety have been discussed in this chapter. The quality of data cannot be taken in isolation but is related to the software and hardware resources involved. This requires whole system dependability to support the decision making process and ensure that risks to patients are minimised. With safe systems, reliable information needs to be available to authorised users in a timely manner, and that supports the decision making process and improves the quality and safety of health care.

As discussed earlier, EHR systems involve processes from data entry to information retrieval. There are challenges in data entry as accurate data is important for data quality. Information retrieval can be either through data displayed on the screen, documentation, discharge referral and event summaries – none of which can be compromised.

To improve the safety of EHRs, potential system errors need to be identified. As in all information systems, EHR systems incorporate software, hardware and people – in other words, system users. Preventing active and latent failures would prevent undesirable consequences from occuring. The literature on patients safety mainly focuses on preventable human errors (e.g. Battles and Lilford 2003; Pronovost et. al. 2003; Gosbee 2002 and Weinger and Slagle 2002) and organization culture (Singer et. al. 2003; Nieva and Sorra 2003). There is a lack of literature regarding technicality errors and risks of EHRs. This research has filled the gap in the patient safety literature by identifying appropriate safety

attributes of EHRs. Determining the safety attributes gives the foundation for performing risk assessment of the EHRs.

EHR systems need to maintain patient confidentiality but they should not impede the workflow of health care processes. Patient consent plays a pivotal role in the success of EHR systems. If the general denial with specific consent model is used without a patient's consent, the record may not be accessible and will not support one of the functions of EHRs, namely easy accessibility. It is arguable that people's privacy should be maintained and their rights respected, but that should not undermine the quality of health care. Researchers need patient data in order to undertake the quality research to provide useful knowledge for the future well being of the health care industry. There needs to be flexibility and healthcare providers should able to access data for both medical purposes and research. Therefore, there needs to be a balance regarding maintaining patient privacy and availability of data for medical research for quality healthcare.

In summary, safety attributes have been identified in this chapter. Next, we need to identify the risk assessment method appropriate for EHRs in order to ensure system safety.

CHAPTER FIVE

RISK ASSESSMENT OF ELECTRONIC HEALTH RECORD SYSTEMS

Risk assessment is needed for EHR systems so that undesirable events can be ruled out and prevented by applying appropriate risk management. The safety attributes of EHRs were identified in chapter 4. Risk assessment of an EHR system is needed to identify whether it possess these safety attributes. To perform risk assessment of EHRs, it is necessary to identify the appropriate risk assessment method.

5.1. Introduction

The Oxford Advanced Learner's dictionary defines risk as the possibility of something bad happening at some time in the future, or a situation that could be dangerous or lead to a bad result (Hornby and Wehmeier 1989). Therefore, potential risks needed to be identified and reduced. Sommerville defines risk as the product of the consequence of a hazardous event and the frequency, or probability of its occurrence (Sommerville 2001):

$$\text{Risk} = \text{Probability} \times \text{Consequence}$$

The following are alternate definitions of risk.

> "Risk is a hazard, bad consequences, loss, or exposure to mischance, risk is the probability of a possible unwanted event and the quantity of possible damage"(SFITZ 2003).

> "Risk is the potential consequences of unwanted adverse consequences to human life, health, property, and/or the environment. The estimation of risk is usually based on the expected value of conditional probability of the event occurring, multiplied by the consequences of the event, given that it has occurred" (IACS 1999).

> "Risk is the combination of the frequency, or probability, of occurrence and the consequences of a specific hazard event" (AS/NZS 3931:1998).

AS/NZS 4360:2004 defined risk as

> "the chance of something happening that will have an impact on objectives. A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. Risk is measured in terms of a combination of the consequences of an event and their likelihood"(AS/NZS 4360:2004).

The context of these definitions include the probability of the hazard and consequences from its occurrence and this study has adopted the definition of risk from Sommerville 2001 as described earlier in this section.

Risk assessment of EHR systems is undertaken in the context of threats to safety. In high risk industries, such as the Aviation Industry, flying is assumed to be risky and it is obvious that errors will have a serious impact. Thus there are checklists, standard protocols and procedures to follow and a black box to record flight data. In healthcare, error reporting and the result of error analysis is

viewed as the assignment of blame (Hudson 2003) so tracking and analysis of errors in medicine is difficult.

Air traffic control systems, Nuclear power plants, and Defense and Military aviation systems are considered high risk, safety critical systems. The following sections define safety systems and explain why electronic health record systems should be categorized as safety systems.

5.2. Safety Systems

5.2.1. Safety Critical Systems

A system whose failure may result in injury, loss of life or major environmental damage can be categorised as a safety critical system (Sommerville 2001). Falla (1995) has identified a safety critical system as a system in which a malfunction could result in

a. loss of life
b. injury or illness
c. serious environmental damage
d. significant loss of or damage to property
e. failure of important mission
f. major economic loss

5.2.2. Safety related systems

Safety related software performs or controls functions which are activated to prevent or minimise the effect of a failure of a safety critical system.

‘Safety critical’ and ‘safety related’ are used equivalently or interchangeably in systems, in which malfunction can result in unsafe or hazardous states (Falla 1995)

EHRs involve sensitive patient health data, hence an error or inaccurate information can have an impact on a patient’s health or even life. EHRs should thus be regarded as safety related systems and as such the principles of risk assessment methods for safety systems can be applied to them. The consequences from an error in electronic health data can impact on quality of life. Safety attributes for EHRs were identified from this research in Chapter 4.

As already mentioned in section 1.1., there has been an increasing awareness of errors and more focus on quality and safety of health care, since the publication of “*To Err is Human, Building a Safer Health System*” (Kohn et al 2000). The Agency for Healthcare Research and Quality and The Veterans Affairs National Center for Patient Safety are healthcare foundations focusing on quality and safety of healthcare in the United States. In Australia, the Australian Council for Safety and Quality in healthcare was set up in 2000 and collaborated with the Australian Institute of Health and Welfare in the surveillance of Australian Health System safety (Runciman 2002).

The Institute of Medicine report (IOM2000) pointed out that the extent of harm that results from medical errors is great and errors result from system failures and not human failures. To achieve acceptable levels of patient safety, major system changes would be required (Bates et al 2001). EHR systems are part of more

widespread healthcare systems and it is imperative that errors are not due to the EHRs themselves.

The following are definitions of Patient Safety Event Types (Battles and Lilford 2003).

> **Adverse/Harm Events** are occurrences during clinical care that result in physical or psychological injury or harm to a patient or harm to the mission of the organization.
>
> **No harm events** are events that have occurred but result in no actual harm although the potential for harm may have been present. Lack of harm may be due to the robust nature of human physiology or pure luck. An example of such a no harm event would be the issuing of an ABO incompatible unit of blood for a patient, but the unit was not transfused and was returned to the blood bank.
>
> **Near misses** are defined as events in which the unwanted consequences were prevented because there was a recovery by identification and correction of the failure, either planned or unplanned.
>
> **Dangerous situations** are where both human and latent failure exist that creates a hazard increasing the risk of harm. Information may be collected from individuals familiar with the process of care in organizations about conditions that are highly likely to cause an injury to a patient or patients.

5.3. Levels of risk

As described previously, risk is the product of the frequency of occurrence and its consequences. Thus either decreasing the frequency of occurrence or decreasing its consequences can reduce risk.

All safety systems such as aviation, financial, rail traffic and medical systems require correct functioning of the software to perform their desired task, thus software failure must be reduced to an acceptable level.

The outcome of risk assessment is a statement of acceptability (Sommerville 2001). Acceptability levels can be classified into: ‘intolerable’, ‘as low as reasonably practical’ (ALARP) and ‘acceptable’ (Figure 5.1).

Intolerable risk should be minimized. Systems should be designed in such a way that accidents will not happen, or when they do they will not result in serious outcome.

ALARP or tolerable risk is defined as a risk within a range that society can live with so as to secure certain net benefits. It is a range of risk that is not regarded as negligible or as something that could be ignored, but rather as something that should be under review and reduced still further (ICOLD 2002).

Acceptable level means the risk is so low that the public will accept that it is not worth reducing the risk further.

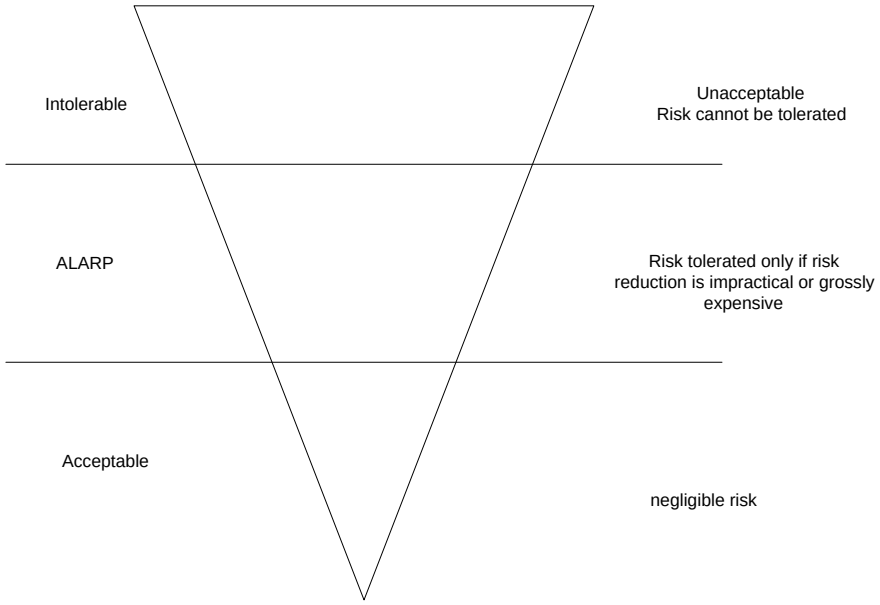

Figure 5.1: Acceptability levels

A level of risk that is acceptable to the general public is ALARP and any system installed should be at least lower than this (Sommerville 2001). Depending on the situation involved, the risk may be different and the acceptability level may differ. Acceptable risk is the highest level of risk associated with a situation that is justifiable. Therefore acceptable risk is a measure of safety.

Example illustrations of acceptability levels for electronic health record systems are shown in table 5.1.

Identified risk	**Probability**	**Severity**	**Estimated risk**	**Acceptability**
Wrong dosage	Medium	High	High	Intolerable
Unnecessary repetition of test	High	Low	Medium	ALARP
Late diagnosis	Medium	Medium	Medium	ALARP
Wrong address	Medium	Low	Low	Acceptable/ALARP
Wrong blood group	Low	High	High	Intolerable

Table 5.1: Example acceptability levels of electronic health records

Wrong dosage

As described in Table 5.1, the probability of the wrong dosage given to the patient may be medium but the severity may be high; and the estimated risk will be high and acceptability level is intolerable. It should also be noted that risk of wrong dosage for different medications could be different. Some risk can be traced back using fault tree analysis as there can be different conditions leading to the risk. Fault tree analysis is discussed in section 5.4.1.1.

Unnecessary test repetition

If the full record is not available or data is lost or the detailed information not available, there could be unnecessary repetition of a test. Acceptability level may also vary according to the test that is to be repeated.

Some tests are not invasive and they may not constitute a great risk to the patient. In that situation, the acceptability level may be ALARP. However, if a test of an invasive nature is to be repeated, there could be severe consequences to the patient.

Late diagnosis

Severity of risk for late diagnosis will also depend on the condition or disease that the patient is suffering from. Risk of late diagnosis for benign conditions may not be that high compared to the risk of malignant conditions, as late diagnosis for the latter can have a catastrophic impact on the patient. Although it may be benign, some medical conditions can have severe consequences. For example: a peptic ulcer may be a benign condition and some patients may have

only discomfort, indigestion or stomach pain, but some can have more serious consequences, such as gastrointestinal bleeding, anterior perforation to stomach or posterior penetration to the pancreas.

Wrong address

In general, the impact of wrong addresses in the medical record for the patient is low as the patient can be contacted by other means. However, if the patient has a life threatening condition and cannot be contacted, the risk may be higher. Therefore, depending on the case, consequences may differ. If the patient has a communicable disease but their address is wrong and if the patient location is not known, there can be a risk to public health.

Wrong blood group

There can be a life threatening condition if a different blood group is given because of error in the data, and acceptability is therefore intolerable.

Therefore, possible errors should be identified and prevented. Potential errors from the system should be identified and analysed based on the severity and frequency of occurrence. Depending on the situation and system requirements and organization, the severity and frequency of hazards may vary. Categorisation of risk for EHRs is different from other risk assessment. The following is an example of categorizing severity and frequency of hazards from other industries:

Catastrophic: involving a large number of deaths, disabling injuries or extensive environmental damage.

Critical: involving few deaths, disabling injuries or more limited environmental damage

Marginal: involving minor injuries and /or local environmental damage.

Negligible: involving damage to the process, plant or product, resulting in economic loss.

The frequencies of occurrence may be described as

Frequent: many times per year.

Probable: once a year

Occasional: once during the lifetime of a system.

Remote: unlikely to occur but require consideration

Improbable: unlikely to occur.

In public health domain, severity of hazards is classified based on the effect on the population. However, severity of hazards determined in the public health domain cannot be applied to electronic health record systems as public health risk is targeted to the population in general and not to the health of individuals.

5.4. Risk Analysis

There are two basic approaches to risk analysis - namely quantitative or qualitative. Quantitative risk analysis is a mathematical approach; qualitative risk analysis involves ranking risk into 'high', 'medium' and 'low' based on knowledge and judgment (Nosworthy 2000). This research adopted a qualitative risk analysis method, as system safety risk analysis is more suited to qualitative approaches (Leveson 2003).

Some analysis techniques that could be used are (Leveson 1995):

- Root cause analysis
    - Fault tree analysis,
    - Management oversight and risk tree analysis,
    - Event tree analysis,
- Hazards and Operability analysis (HAZOP),
- Failure Modes and Effects Analysis (FMEA),
- Failure Modes, Effects and Criticality Analysis (FMECA) and
- Task and Human Errors analysis

Both risk assessment and risk analysis have been described in the literature as developing an understanding of risk in order to provide an input to decisions on whether risks need to be addressed and the most appropriate and cost-effective risk treatment strategies (Sommerville 2001, Leveson 1995, AS/NZS 4360). Therefore, both are used synonymously in this thesis.

Risk analysis in the process industry can be identified into seven stages, namely system description, hazard identification, incident enumeration, incident frequency estimation, consequence estimation, evaluation of consequences and risk estimation (Cox and Cox 1996).

Risk analysis of electronic health record systems includes:

<u>System description</u>

System description identifies and describes the system to be analysed. As different healthcare institutions use different EHR systems, analysis differs from one to another.

Hazard Identification

Risk will differ according to the system, as there are different processes involved for different systems.

Incident frequency determination estimates the frequency of the event occurring.

Consequence determination determines the potential for damage or harm from the specific incidence.

Evaluation of consequences

This estimates the frequency data of specific consequences. As EHR systems are only in their infancy stage, it is difficult to evaluate the consequences of risks from electronic health record systems. However, the consequences of specific conditions and possible outcomes will be discussed in section 5.4.6.

Risk estimation is the product of the likelihood and the consequence of risk.

5.4.1. Root Cause Analysis

This is the most basic cause that can be reasonably identified and that management is at liberty to fix (Livingston et al. 2001).

5.4.1.1. Fault Tree Analysis

This is the most widely used method in system reliability analysis. It is a deductive top - down method of analysing system design and performance. Fault tree analysis involves system definition, fault tree construction, qualitative analysis and quantitative analysis. It involves specifying a top event to analyse, followed by identifying all of the associated elements in the system that could cause the top event to occur (Relex Software Corporation 2001). The following examples are fault tree analysis for adverse drug reactions; hypersensitivity to

drug and wrong dose of medication. As seen in the example fault trees of Figures 5.2 and 5.3, the top event - adverse event wrong dose, and hypersensitivity, respectively - can be traced back to the bottom nodes. In other control systems, failure or hazardous events are machine failures, either from software or hardware causes.

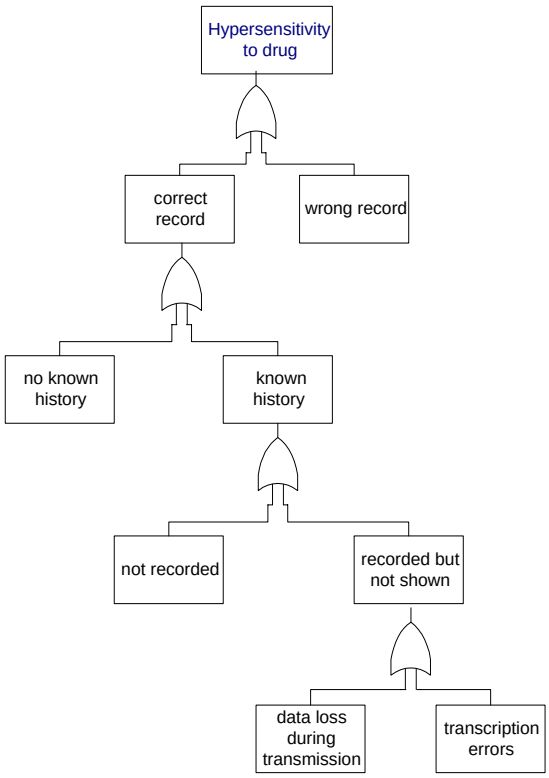

Figure 5.2: Fault tree analysis of Hypersensitivity to drug

Drug hypersensitivity can be traced back for errors. It can happen to patients with no known history of drug hypersensitivity, or if there is a known history of hypersensitivity but this could either be recorded in the medical record or was recorded but not shown due to data loss or errors.

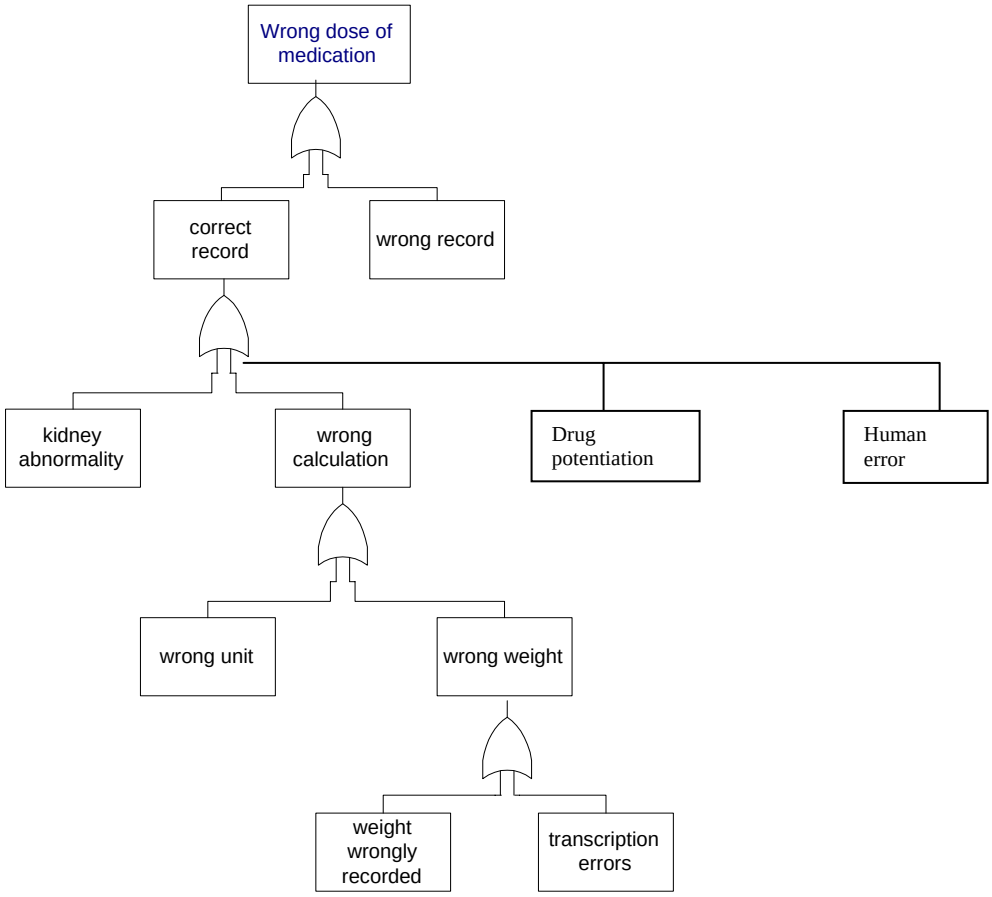

Figure 5.3: Fault Tree: Wrong dose of medication

The event “wrong dose of medication” can be traced back to root causes. It can be due to medication administered to the wrong patient by referring to the wrong record, or it could be a correct patient with the correct record but due to a different condition. It can be due to a patient with kidney abnormalities where the drug dosage should be lowered, or it could be due to drug potentiation, due to drug combination effects or it may be due to human error or wrong dosage calculation, - for example, an error in the unit or because of the wrong weight. For every adverse effect errors can be either technical or human.

5.4.2. Management Oversight and Risk Tree Analysis

This was developed in the 1970s for the United States Nuclear Regulatory Agency. It is a standard fault tree augmented by an analysis of managerial functions, human behavior and environmental factors (Leveson 1995).

5.4.3. Event Tree Analysis

This is a decision tree technique, which uses forward search to identify various possible initiating events by determining all sequences of events that could follow. The states in the forward search are determined by the success or failure of other components (Leveson 1995). The goal of the event tree is to determine the probability of an event based on the outcomes of each event in the chronological order of the events leading up to it (Relex Software Corporation 2001). Figure 5.4 is an example of event tree analysis for failure to access a health record. As demonstrated in Figure 5.4, both the probability of accessing the record and failure can be determined by the event tree. Therefore, quantitative analysis can be performed if there are previous known failures and probabilities.

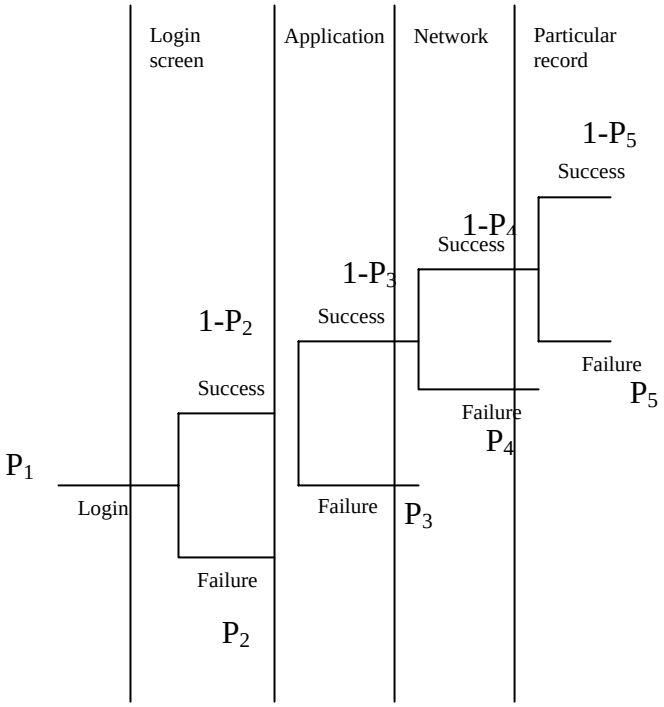

Figure 5.4: Event tree analysis for failure of access to health records

Failures can be from different states. It could be failure in the login screen, failure in the application, failure in the network, failure to access the particular record. As shown in figure 5.4., the probability of failure to login is P_2, the probability of successfully logging into the screen will be $1\text{-}P_2$. Likewise, if the probability of application failure is P_3 the success would be $1\text{-}P_3$. Therefore, the probability of successful access to the particular record (P_x) can be calculated as:

$$P_x = P_1 (1\text{-}P_2) (1\text{-}P_3) (1\text{-}P_4) (1\text{-}P_5)$$

To calculate this, the probability of success or failure should be known. Therefore, quantitative analysis can be performed if there are previous known failures and probabilities. The aim of risk assessment of EHR is to prevent error; analysis through known failure is not appropriate for this study. The study aims to predict possible failures *before* they happen and prevent them. Therefore, event tree analysis is ruled out as a suitable risk assessment method for electronic health record systems.

5.4.5. Hazards and Operability Analysis (HAZOP)

HAZOP is a qualitative analysis technique. The purpose of which is to identify all possible deviations from the design's expected operation, together with all hazards which are associated with these deviations. Therefore, HAZOP is appropriate to elicit hazards in new designs and hazards that have not been considered previously. Thus, it is more appropriate for software development risk and is not suitable for this study, as it relates to *new* systems, not evaluation of an existing system.

5.4.6. Failure Modes and Effects Analysis (FMEA)

FMEA was developed by reliability engineers to predict equipment reliability. It is a form of reliability analysis that emphasizes successful functioning rather than hazards and risks. It detects the overall probability that the product will operate without failure for a specific length of time. FMEA is a process for identifying the effects associated with individual failures within a system (Marx and Slonim 2003).

The United States Veterans Affairs National Center for Patient Safety (NCPS) has identified the basis of FMEA as being prevention of tragedy, as well as to make systems more robust and fault tolerant. NCPS has identified that if FMEA were utilized, major medical center power failure, MRI incident- ferromagnetic objects, bed rail and vail bed entrapment and medical gas usage might be recognized and prevented (VHA NCPS 2003). We therefore need to identify whether FMEA could be applicable to electronic health record systems.

Healthcare failure Mode and Effect Analysis includes

1. A prospective assessment that identifies and improves steps in a process thereby reasonably ensuring a safe and clinically desirable outcome
2. A systematic approach to identifying and preventing product and process problems before they occur (VANCPS 2003)

To determine the FMEA, the severity and probability of the potential failure mode needs to be identified and worked out with the FMEA decision tree.

Hazard Analysis

Hazard analysis is the process of collecting and evaluating information on hazards associated with the selected process. The purpose of hazard analysis is to develop a list of hazards that are of such significance that they are reasonably likely to cause injury or illness if not effectively controlled.

Failure Mode

Refers to the different ways that a process or sub-process can fail to provide the anticipated result.

As discussed in Chapter 3, EHR systems involve processes that range from data entry to decision making. For example, the outcome “wrong test result” can occur from errors in different steps in the processes involved in the ordered test. Figure 5.5 illustrates the processes involved in a laboratory test. The laboratory test ordered can be divided into 1. test ordered, 2. draw sample, 3. process sample, 4. reporting and 5. filing results. These processes can be subdivided into sub processes as shown in figure 5.5. Possible failure modes from these processes are shown in Figures 5.7 through 5.10.

For FMEA, the potential failure mode for each process can be identified as follows:

For example, for the laboratory test processes will include:

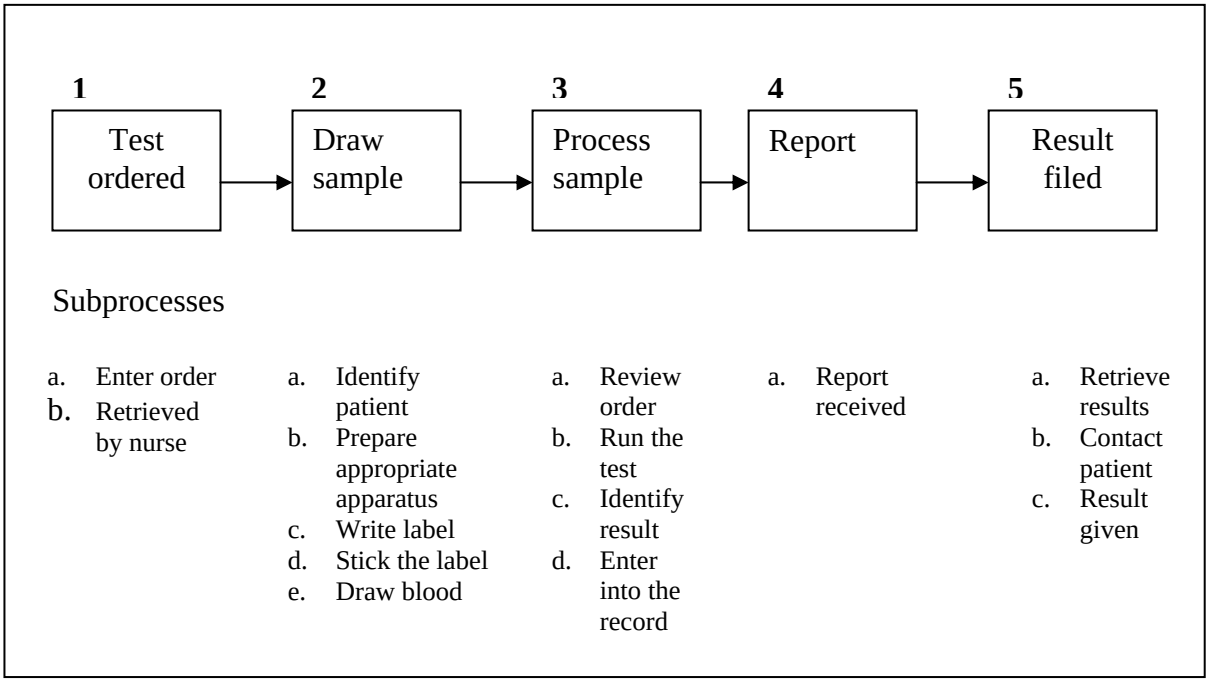

Figure 5.5: Processes involved in the laboratory test

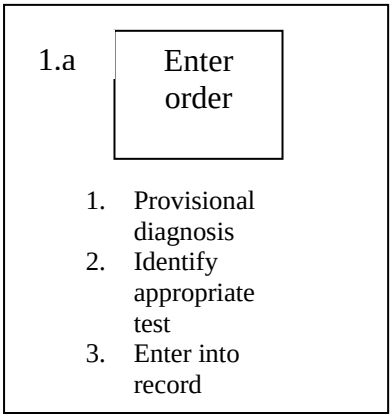

Figure 5.6: Subprocesses of Process 1a. "Enter order"

Failure mode

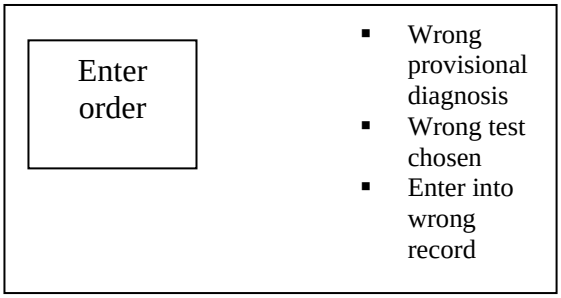

Figure 5.7: Failure mode of "Enter order"

Failure mode

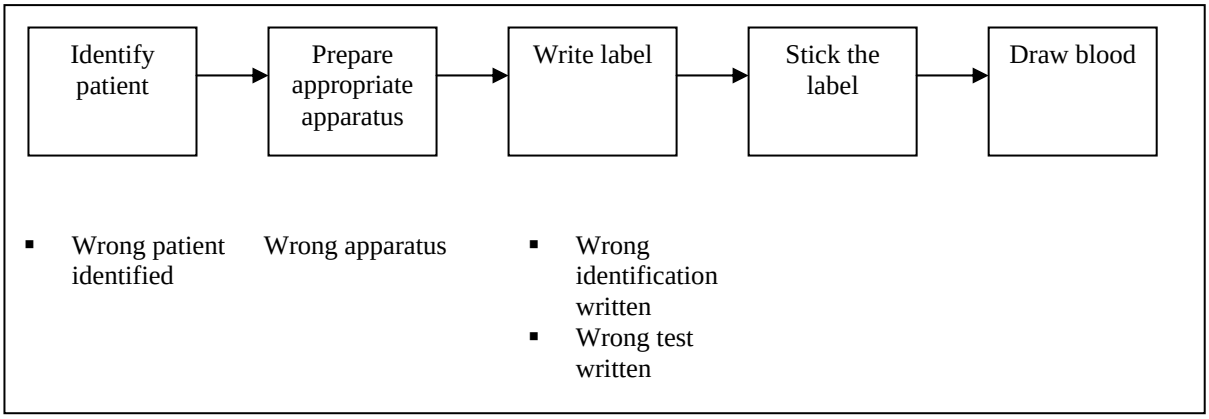

Figure 5.8: Failure mode for process 2 (Draw Sample)

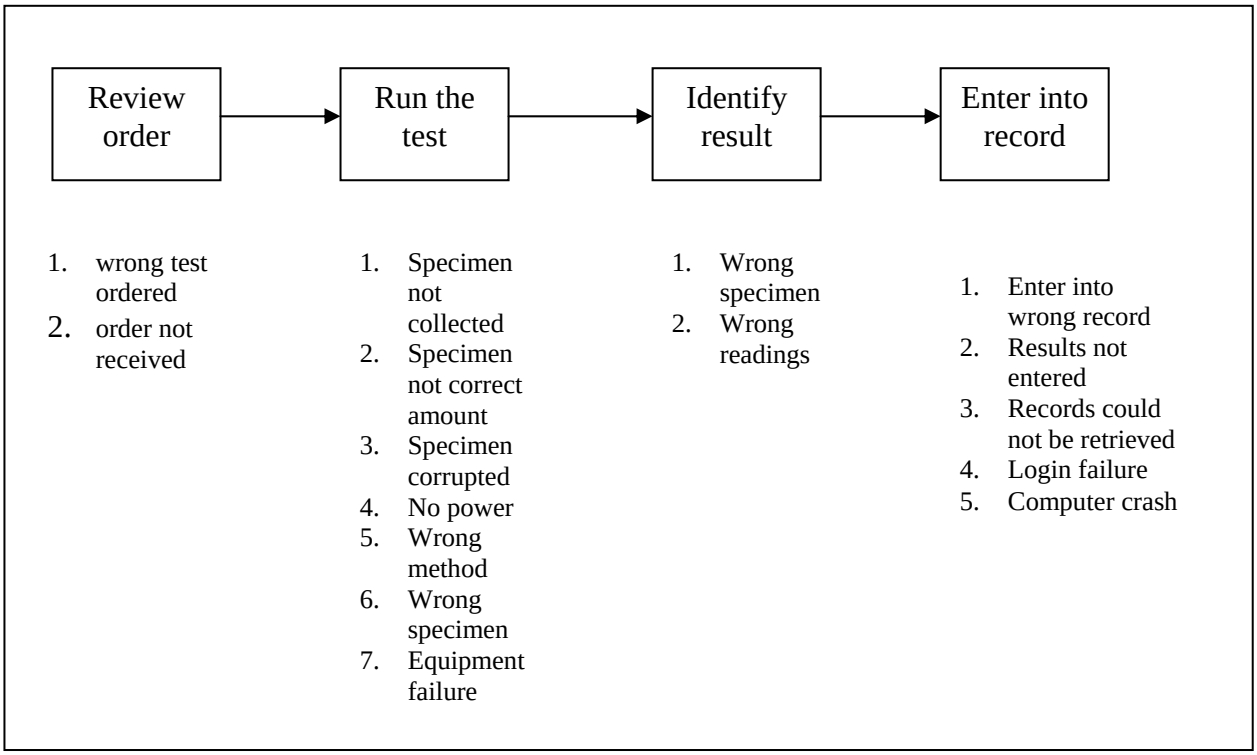

Figure 5.9: Failure mode for process 3 (Process Sample)

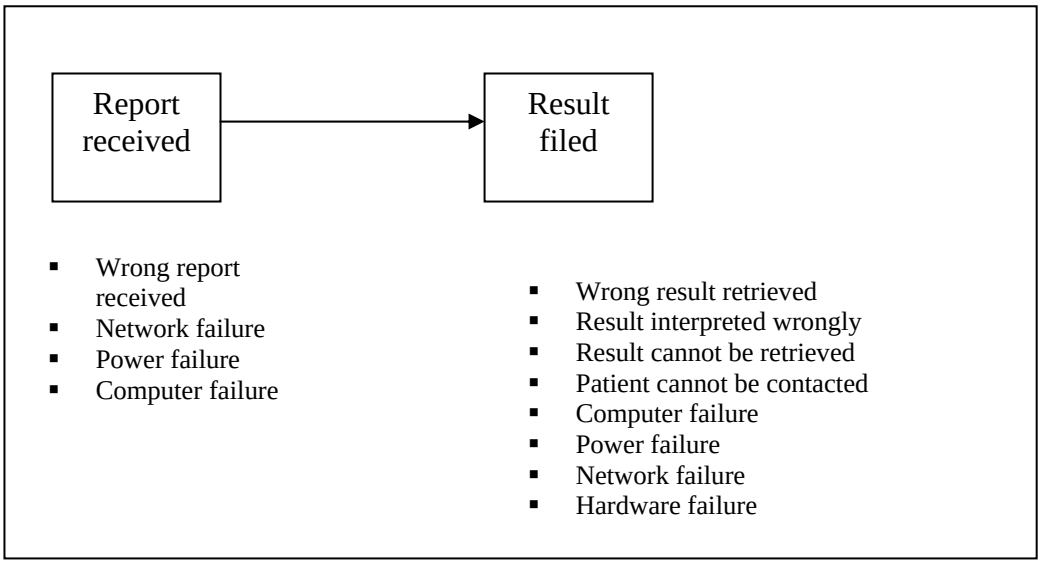

Figure 5.10: Failure mode for processes 4 (Report) and 5 (Result filed)

Figure 5.11 is a possible subprocesses involved in the medication given to the patient. Possible failure modes of these processes can be predicted and the level of risk identified accordingly.

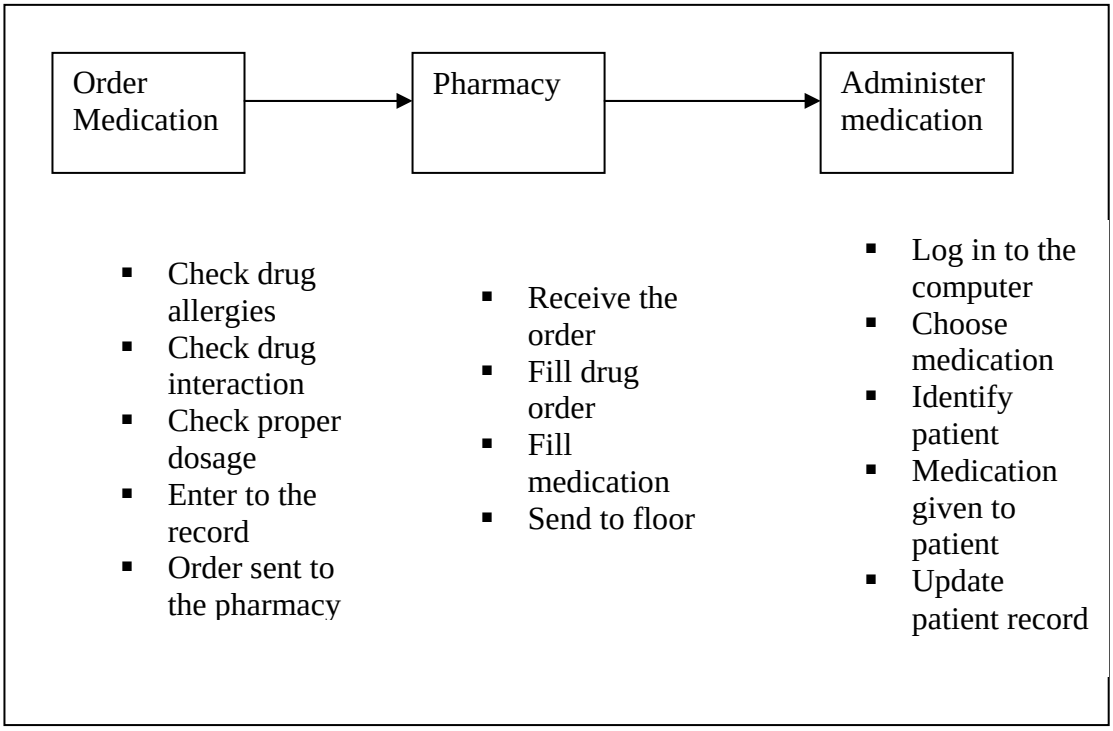

Figure 5.11: Processes involved in giving medication

Decision Tree of failure mode

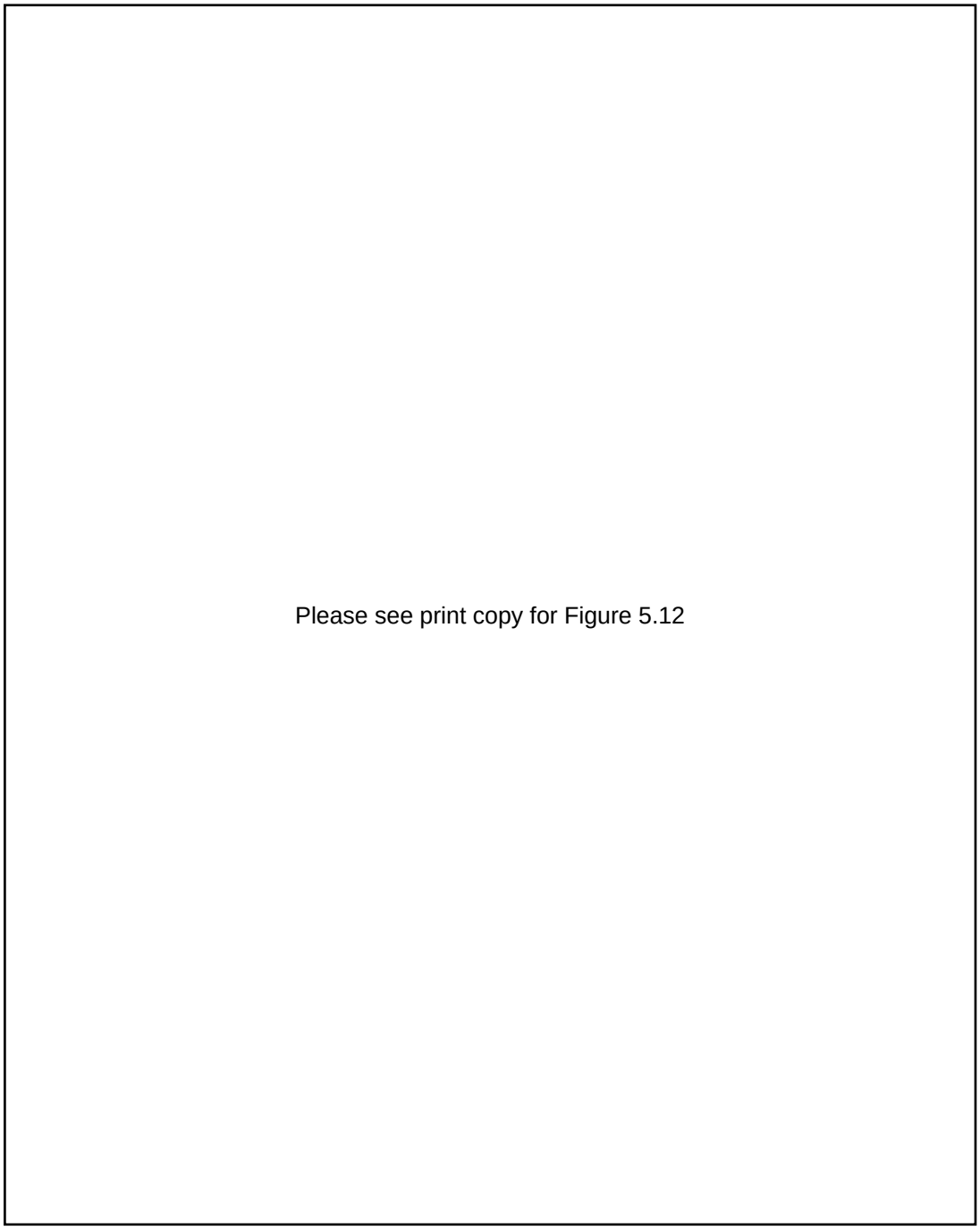

Figure 5.12: Decision tree for FMEA (VA National Centre for Patient Safety 2003)

5.4.7. Scenario Analysis

The following scenarios are analysed with a view to determining the appropriate risk assessment method for each.

Erroneous record

Erroneous records could result in misidentification, false test results, wrong diagnosis and wrong treatment.

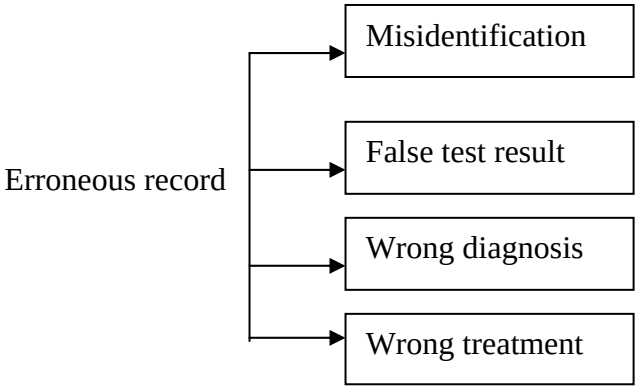

Figure 5.13: Erroneous record

Misidentification

Misidentification of the patient could be due to the wrong identifier, the system not working properly, loss of record or the system being down at the time of request.

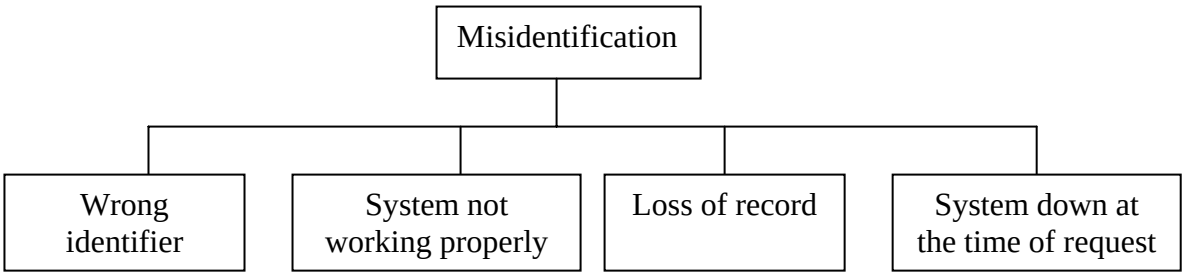

Figure 5.14: Misidentification

Wrong Treatment

Wrong treatment could be the result of wrong diagnosis, which in turn could be due to wrong record, loss of data, or modification of data.

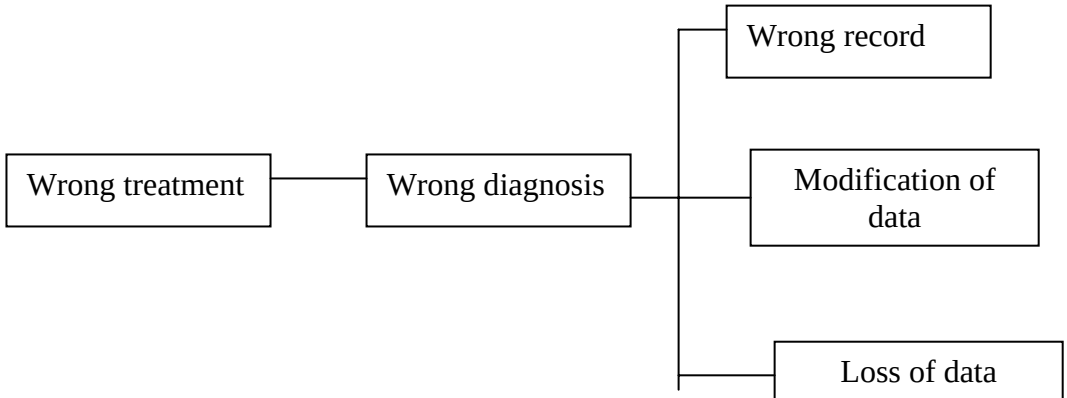

Figure 5.15: Wrong treatment

It can be noted that “erroneous records”, which is one of the possible failure modes of the system, from that probability of possible adverse events can be identified as shown in Figure 5.13. Preventing or reducing errors in records can decrease possible failures. In the scenario, “Misidentification of patient”, the patient has already been misidentified. There may also be consequences from the result of misidentification. Therefore, it indicates that the event has happened and the root causes of why that event has happened can be traced back. If it was the

“near miss event” or “no harm event”, identifying base events or root causes could reduce future failures by preventing them. However, if the event has happened and if there is an adverse event or a dangerous situation, tracing back with fault tree analysis could not reduce the damage that has already occurred. “Wrong treatment” could be analysed with backward analysis. It can either be from technical failure or human error. As this research focuses on identifying errors due to electronic health record systems, human errors will not be explored further.

5.4.8. Framework for the risk assessment of EHRs

The framework for the risk assessment of EHRs can be deduced by analysing examples from section 5.3 and the case scenarios described in section 5.4.7. It is concluded that the framework for the risk assessment of EHRs should include:

1. Identifying the probability of risk of EHRs
2. Identifying the consequences from the specified risk
3. Identifying the acceptability level of risk
4. Development of mitigation plan according to the level of risk

Table 5.2 identifies whether the attributes 1-4 identified in the risk assessment of EHRs framework can be fulfilled by the different risk assessment methods.

	1	2	3	4	Comments
FTA	Yes	Yes	Yes	No	Mitigation plan for future risk is possible but not for current risk
ETA	No	Yes	Yes	Yes/ No	Probability can be calculated by quantitative analysis through known failures
HAZOP	NA	NA	NA	NA	used for system development
FMEA	Yes	Yes	Yes	Yes	

Table 5.2: Relationships between Risk assessment methods and the Framework

Therefore, it can be seen that FMEA is the most appropriate method for the risk assessment of EHRs.

5.5. Chapter Summary

This chapter discussed why EHR can be categorized as a safety system and explained the acceptable level of risks of EHRs by way of different examples. Critical analysis of various risk analysis was carried out and discussed. As stated in Chapter 1, there is currently *no* published literature regarding risk assessment of EHRs. This study has analysed the applicability of different risk assessment methods to EHRs. Various scenarios were examined and the suitable risk assessment method for EHRs identified.

Failure Mode Effect Analysis was identified as the appropriate EHR risk assessment method since it involves identifying possible system failure modes *before* actual failure, and thus could mitigate the future occurrence of errors. By contrast, in root cause analysis - such as fault tree analysis - the source of error is identified *after* the incident occurs. Therefore, fault tree analysis is suitable for retrospective studies, where adverse events or errors have occurred and to track back to the root cause conditions.

With FMEA, failure modes can be predicted and in principle be prevented from occurring. It is important to first identify possible risks to ensure safety, so FMEA is more suitable compared to root cause analysis. Accordingly, the risk assessment case studies reported in this thesis were all conducted using FMEA.

In summary, this chapter has identified the appropriate risk assessment method for EHRs. The stage has now been set for an empirical study applying the identified risk assessment method and identified safety attributes of EHRs within various health care organizations.

CHAPTER SIX

Methodology

This study explored the suitability of different risk assessment methods suitable for electronic health record system. The research questions set out for this study are (i) How can the safety of EHRs be measured? and (ii) What are the safety attributes for EHRs? To answer these questions, a framework for safety assessment of EHRs has been developed by

- Identifying a theoretical basis of safety, based on dependability and data quality,
- Defining the safety components of EHRs,
- Identifying a risk assessment method applicable to EHRs,
- Evaluating this risk assessment method, and
- Drawing conclusions based on the above findings

Risk assessment case studies were conducted on EHRs from two different health care institutions after identifying the appropriate risk assessment method from this study. These case studies were conducted to validate whether the identified risk assessment method is applicable to the safety assessment of EHRs.

6.1 Research Plan

The overall aim of this research was to answer the research questions posed at the start of this chapter. The research plan is outlined in Figure 6.1. The theoretical basis of the study is derived from:

1. an understanding of EHRs,

2. an analysis of failures of healthcare computer systems,
3. identification of the safety attributes of EHRs, and
4. identification of the appropriate risk assessment method for EHRs

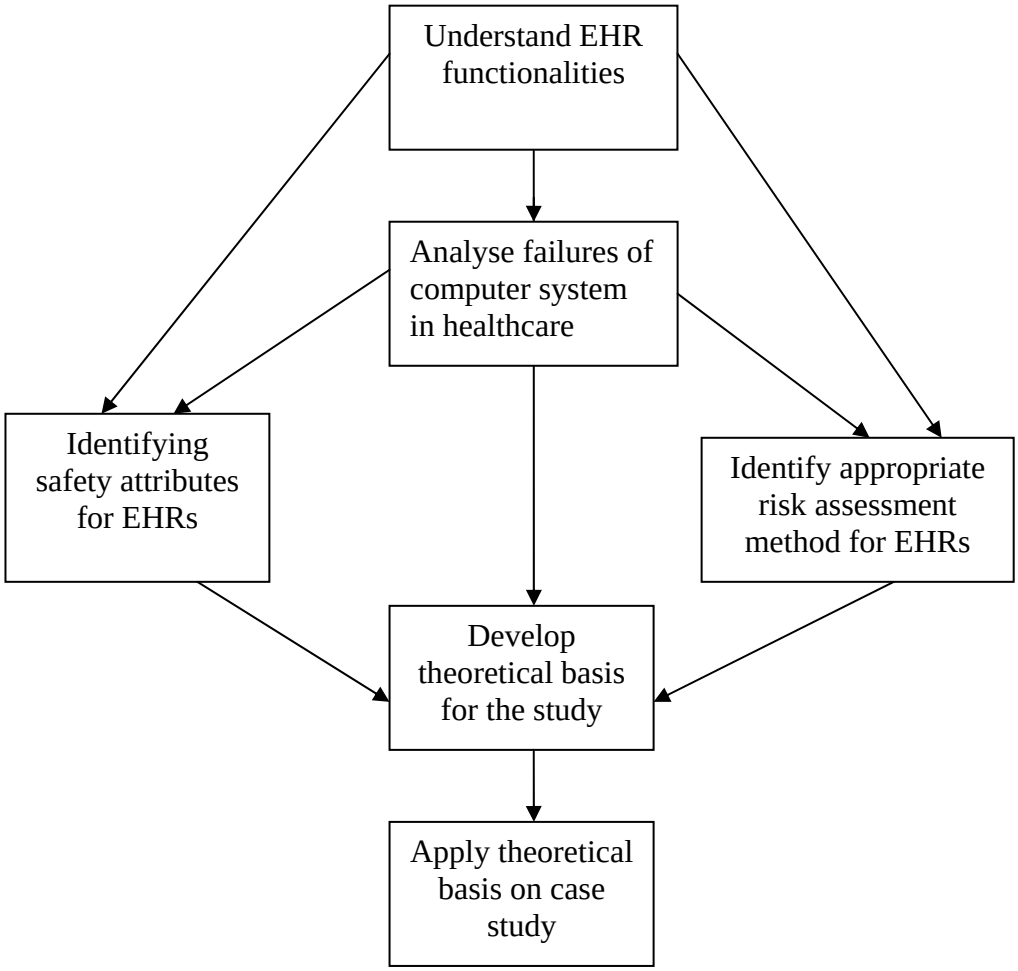

Figure 6.1: Research Plan

The research methodology is mainly of a qualitative nature, as this project involved a selected group of subjects, locations and situations to be observed and interviewed, and focused on what is going on in specific settings (Bouma 1996). Moreover, as discussed in Section 5.4, qualitative analysis is more appropriate for the risk assessment study. In addition, qualitative research is appropriate for the research, when the topic is new, the topic has never been addressed with a

certain sample or group of people, or existing theory does not apply to the particular sample under study (Creswell 2003). In contrast, quantitative methods include questionnaires, surveys, experiments and content analysis with data in numerical form to test a theory or established phenomenon (Creswell 1994). As there is *no* risk assessment methods currently exist for EHRs, qualitative assessment method is a suitable method for this study. Therefore, qualitative risk assessment method was adopted in this study. After developing a theoretical framework, the concept of EHR risk assessment needs to be investigated within a real life context by way of case studies.

Following research designs can be involved in research process (Bouma 1993).

1. The case study
2. The longitudinal study
3. The comparison
4. The longitudinal comparison
5. The experiment.

The case study has been identified as a building block of research design to study a variable or sets of variables measured at one point of time. The Longitudinal study follows the period of time and finds out whether there were any changes during that time. Comparison involves comparing one group to another. The longitudinal comparison involves comparing two or more groups in a period of time. The experiment involves determining the effect of a change in one variable over another (Bouma 1993). Case study design has been selected based on the nature of the data required for this study,

Case study research also has been identified as the most common qualitative method used in information systems (Myers 1997) and it is an ideal methodology when in-depth investigation is needed (Tellis 1997). This study utilised the case study method as it is an empirical inquiry that:

- investigates a contemporary phenomenon within its real-life context, especially when
- the boundaries between phenomenon and context are not clearly evident (Yin 2002)

6.2. Case Study Design

Research questions of this research are "How can the safety of EHRs be measured?" and "What are the safety attributes of EHRs?" The theoretical background of EHRs was established and their safety attributes identified in Chapter 4. Yin (1994) has emphasised that theory development of the case study is highly important. Theory development of this study was by establishing the safety attributes for EHRs and identifying the most appropriate method for risk assessment of EHRs in Chapter 5. The purpose of case studies is to demonstrate that safety of EHRs can be measured by the FMEA (Failure Mode Effect Analysis). The unit of analysis for this case study is EHRs. Field studies for case studies were conducted for over one and a half year period and data collected from EHRs were analysed, linked back with the safety attributes identified and interpreted to prove that the research question has been answered.

Case studies were conducted after identifying the research methodology, which includes the development of a theoretical framework (Chapters 2 through 4),

identifying the safety attributes of electronic health records (Chapter 4), and identifying suitable risk assessment methods for EHR systems.

6.3 Data collection

Data collection is through the use of documented systems data, test data and information from system users and administrators. Stake (1995) has identified two principles used in case studies as to obtain the descriptions and interpretations of others (Stake 1995).

Following methods of data collection were conducted in this study.

6. Observation
7. Interviews
8. Document Reviews
9. Questionnaires

6.3.1 Observation

Observations were used in this study to understand the system processes involved. This helped to identify the workflows involved as well as the potential system risks.

6.3.2. Interviews

Information regarding systems was gathered through informal interviews and feedback from users. Data collection was performed by way of informal interviews. Richer information could be obtained through open-ended interviews which also reduces misleading conclusions from questionnaires and close-ended questions (Boynton and Greenhalgh 2004). Nevertheless, feedback from

clinicians was obtained through the combination of preset questionnaires and open ended questions in this study. Questions were used to obtain information as they were short and focused. Open-ended questions were also included to identify issues not covered in the closed questions. Hence, it discovers the questions unsolved and experiences and expressions from the interviewees. Therefore, this study embraces the fieldwork by observing how the system works and getting information through interviewing users, system administrators and getting feedback from users.

6.3.3. Document reviews

System documents, user manuals, training materials, records of test data, privacy and policy manual, technical manuals, documents containing information related to systems were reviewed to obtain a richer data source for the study.

6.3.4. Questionnaires

Although questionnaires are quantitative in nature, this study involved questionnaires and open ended questions to obtain feedback from busy clinicians to obtain important information regarding the process and the workflow involved in the system to complement observations in Section 6.3.1. Although questionnaires were based on the Likert scale of strongly agree to strongly disagree, these were not statistically significant as there were only 14 correspondents involved. However, this group represents expert users of the system who have knowledge of the nature of risks being studied.

6.4. Case studies approach

Case studies conducted involve continuous interaction between the theoretical issues such as functionalities of EHRs, safety attributes, risk assessment methodologies and the information being collected. House (1980) classified case study evaluation into eight approaches, four of which are 'objectivist' and the remaining four 'subjectivist': alternatively it is referred to as 'interpretivist' approaches by Travers 2001, Yin 1994 and Stake 1995.

(a) The objectivist approaches are (Friedmann and Wyatt 1997):

1. Comparison-based

   In comparison-based approach, the information resource under study is compared to a control condition, or a contrasting resource

2. Objectives-based

   Objectives-based approaches determine if a resource meets its designers' objectives

3. Decision facilitation approach

   In this approach, the evaluation is targeted to resolve important issues to developers and administrators, so they can make decisions about the future of the resource

4. Goal free

   In this approach, the evaluation is conducted as purposefully blinded to the intended effects of the resource.

(b) The subjectivist (interpretivist) approaches are

1. Quasi legal,

In this approach, a resource under study is judged as a mock trial, or through other formal adversary proceedings.

2. Art criticism,

In this approach, an experienced person in the field or who has a great deal of experience with a resource works with the resource over a period of time and writes a review highlighting the benefits and limitations of the resource.

3. Professional review

This is the site visit approach for evaluation; site visits are often guided by a set of guidelines specific to the type of project under study but sufficiently generic. Friedmann and Wyatt (1997) have recommended that evaluation of computerised patient records fall under this category.

4. Responsive/Illuminative (Friedman and Wyatt 1997; House 1980).

This approach represents the viewpoints of users of the resource. The goal is understanding or illumination, rather than judgement. The study begins with a minimal set of orienting questions.; deeper questions are set throughout the project as it evolves.

The case studies analyse whether the system meets the safety attributes previously identified in this research, and involves site visits, understanding how the system works, identifying system sub-processes, identifying failure modes, giving feedback to users, and system review through meetings and feedback. Accordingly, the study uses a combination of the Art Criticism, Professional Review, and Responsive/Illuminative approaches. Feedback is important for administrators and users to resolve system issues, so the study also incorporates

the decision facilitation approach. Therefore, the study uses a combination of both objectivist and subjectivist approaches (Figure 6.2).

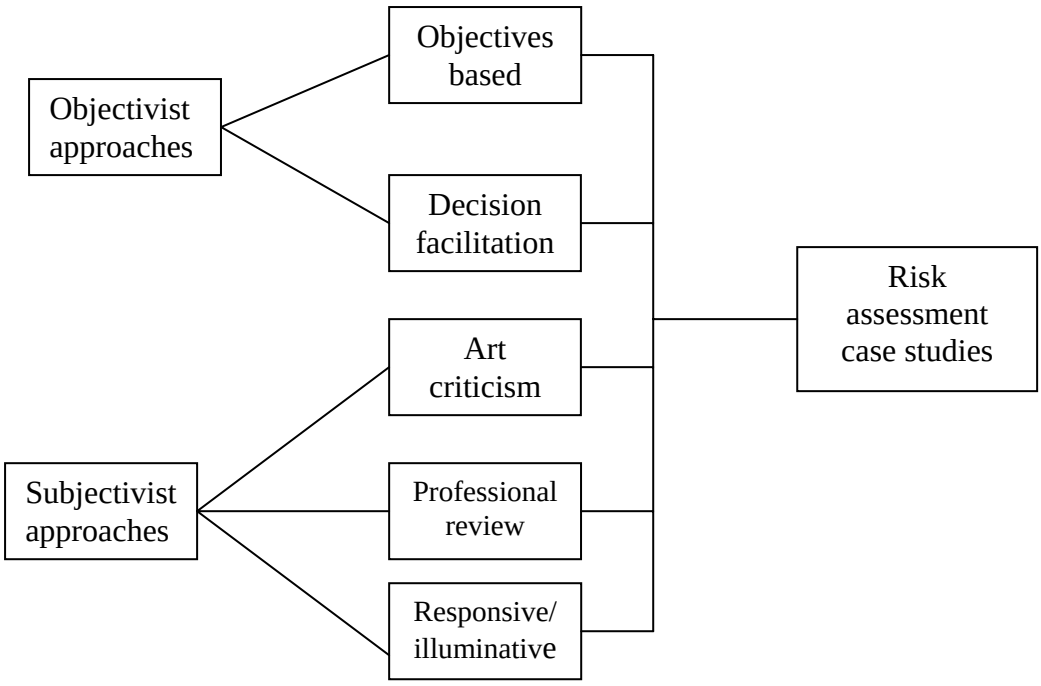

Figure 6.2: Approaches used in the risk assessment case studies

6.5. Case studies and their significance

Case studies use multiple sources of evidence to obtain accurate results. The use of multiple sources of evidence allows addressing a broader range of historical, attitudinal and behavioural issues. Thus, any findings or conclusions in a case study are much more likely to be convincing and accurate, as they are based on several sources of information (Yin 1994).

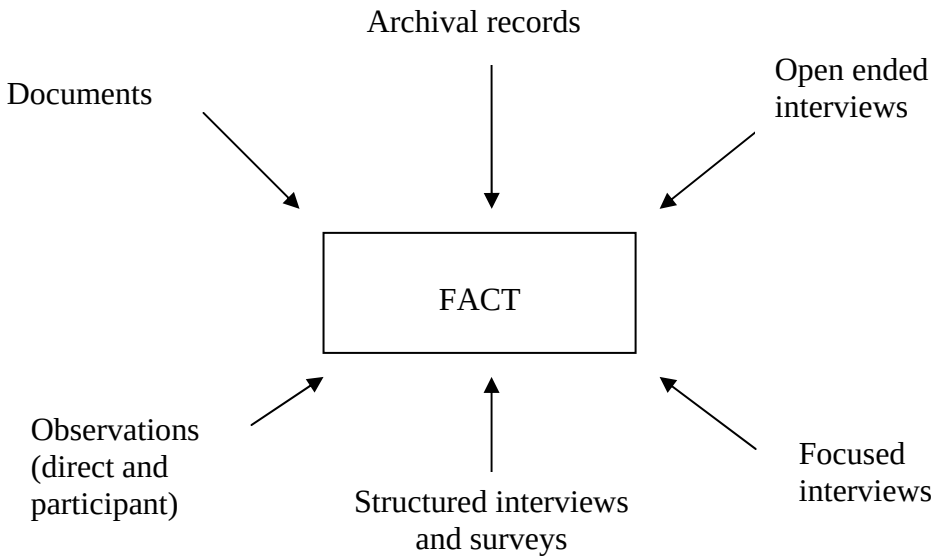

Figure 6.3: Convergence of multiple sources of evidence: Single study (Yin 1994)

Figure 6.3 illustrates the attributes involved in forming convergence of multiple sources of evidence. The case studies conducted as part of this research involved such a convergence.

In the Community Health Information Management Enterprise case study, fact gathering was conducted through looking at CHIME user manuals, training package documentation, documentation of CHIME presentations, CHIME business process documents, along with structured and open-ended interviews, clinicians survey/questionnaire, observations of how the system worked, and by walking through the training system. Because of confidentiality, archival records were not available to view, but test data and feedback from users were used to collect comprehensive data.

In the Maternal and Infant Network (MINET), forms, user manual, technical manuals and privacy and confidentiality guidelines were reviewed. The scanning process, data entry and retrieval were also observed. However, only test data were used for reasons of confidentiality. Open-ended interviews, closed interviews and user feedback were all used in this study. As this study involves different variables, uses multiple evidence, triangulation and also uses the theoretical background identified in Chapters 2 through 5, the case study method used in this study ensures validity.

6.6. Analytic Generalizing from case study

Safety attributes were identified and the 'FMEA' risk assessment method used in case studies conducted in two different healthcare settings. In both organisations, electronic health record systems are used in a community healthcare context, however the specific use of data in each case is different; CHIME data is used mainly for primary care, whereas MINET data is used for research purposes.

MINET and CHIME were selected as the case studies as both systems involved electronic health data. CHIME is responsible for primary care and involves data for community health. MINET involves data mainly from community health (maternal and child health) as well as data downloaded from hospitals (obstetrics data). Thus CHIME and MINET cater for technically distinctive purposes and situations. Moreover, different sources of data are used for each case study – this leads to benefit in analysing the proposed theoretical framework of risk assessment for EHR systems. Thus, the results obtained from the MINET and CHIME case studies were analysed against the safety attributes identified in

Chapter Four to establish the theory for this Thesis. Recommendations and improvements to both systems were made based on the results obtained from this research.

6.7. Validity and Reliability

This study utilised an appropriate research methodology according to the literature review and followed closely the case study approach recommended by Yin 1994, Travers 2001, Tellis 1997 and Myer 1997. The study design was based on the literature review, advice from the Health Informaticians in the industry and academics. Further, the risk assessment studies conducted in these two healthcare organisations can be generalised to the EHRs in general (ref. Chapter 7). Finally, data collection methods used in these studies are also appropriate for future studies of a similar nature.

6.8. Chapter Summary

In summary, this chapter justifies the research methodology undertaken in this study. It includes the research plan, objectives of the study, case study design, case study approaches, analytic generalisation from the case study and validity and reliability of the research. The following chapter will present the empirical case studies conducted in the Maternal and Infant Network, Simpson Centre for Health Services Innovative Research, South Western Sydney Area Health Service and Community Health Information Management Enterprise.

CHAPTER SEVEN

CASE STUDIES

The research questions of this dissertation are “How can the safety of EHRs be measured”, and “what is the appropriate method for risk assessment of EHR systems”?

The research was undertaken between 2000 and 2004, with the case studies conducted in 2003 and 2004. The previous five chapters outlined the development of a theoretical framework for the safety of EHR systems and identified an appropriate risk assessment method. This chapter details two case studies conducted in different healthcare settings.

7.1. Introduction

At the start of this research (2000), the National Electronic Health Record Taskforce of Australia proposed a Health Information Network for Australia (HINA) to develop a nationally coordinated and integrated EHR (NEHRT 2000). One of the objectives of proposing the HINA was to ensure consumer safety. The US National Academy Press publication, “To err is human, building a better health systems”(2000) along with the UK NHS publication, “An organisation with a memory” highlighted preventable medical errors and safety (Department of Health Expert Group 2000). Both emphasized the importance of safety and motivated the present study into the safety and risk assessment of the EHR systems.

7.2. Risk Assessment Case study of CHIME (Illawarra Area Health Service)

Safety Assessment of the Community Health Information Management Enterprise is important as CHIME has been identified as one of the foundation EHRs for NSW. The first site for CHIME was in the Hunter Valley. CHIME is designed to cover a wide range of community health settings, and has been described as

> "An operational, clinical information system that has proven to improve service delivery, outcome measures and productivity" (Hornsey and Friend 2003).

An integrated clinical information program of integrated EHRs for NSW has been identified (Figure 7.1).

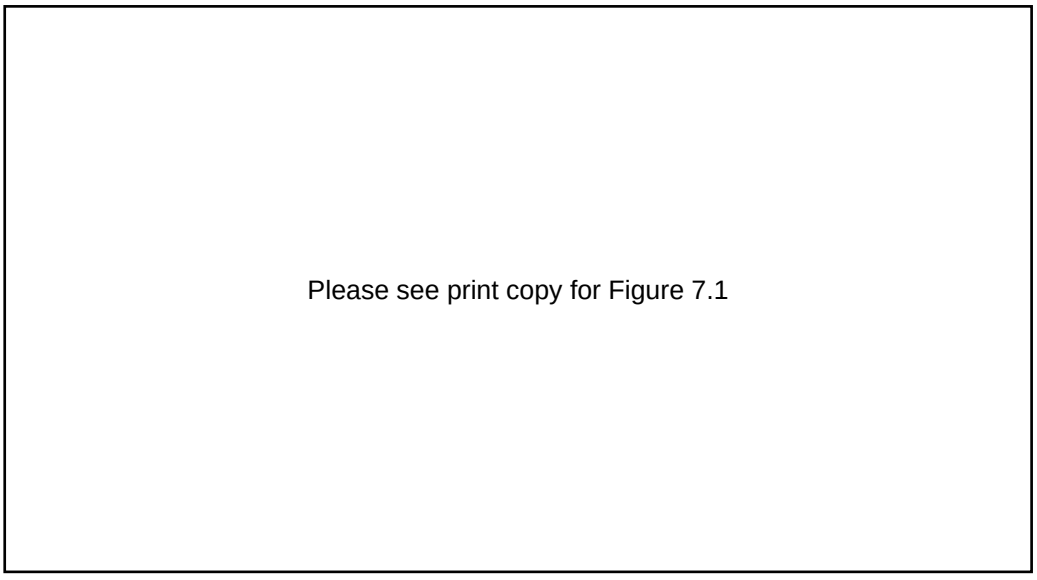

Figure 7.1: Integrated Clinical Information Program (Hornsey and Friend 2003)

There are various community health services and CHIME was developed to cater for 39 of these. Processes involved in CHIME are service request, service contact-diary and management plan. Service requests enable users to view clinical notes, service contacts and alerts across service and treatment episodes. Episode and subsequent service requests are protected by a confidentiality security layer, which only allows individuals with the correct data sharing profile to view information contained in them. CHIME also involves report generation for clients and management.

To conduct risk assessment of CHIME, severity and probability of risks need to be categorised. As identified in Chapter 5, risk assessment of CHIME will be conducted through FMEA.

Severity and probability level is defined as follows:

Probability

Low: rarely or never occurs

Medium: occurs occasionally or a few times per year

High: occurs regularly (e.g. on a weekly basis)

Severity:

Low: data is non-vital, and may be replaced easily; if the information is disclosed, it is not sensitive

Medium: data is important to patient care; information may be sensitive, and can have some impact on the patient

High: data is critical; permanent loss of data, can have a detrimental effect on the patient

Table 7.1. Probability and Severity of risks

Risk/Hazard Score

Severity / Probability	Low	Medium	High
Low	1	2	3
Medium	2	4	6
High	3	6	9

Table 7.2. Hazard Score

To access CHIME, the user needs to first log on to the Health Data Operating Centre and then to CHIME.

The Processes involved in creating a service request within CHIME are shown in figure. 7.2.

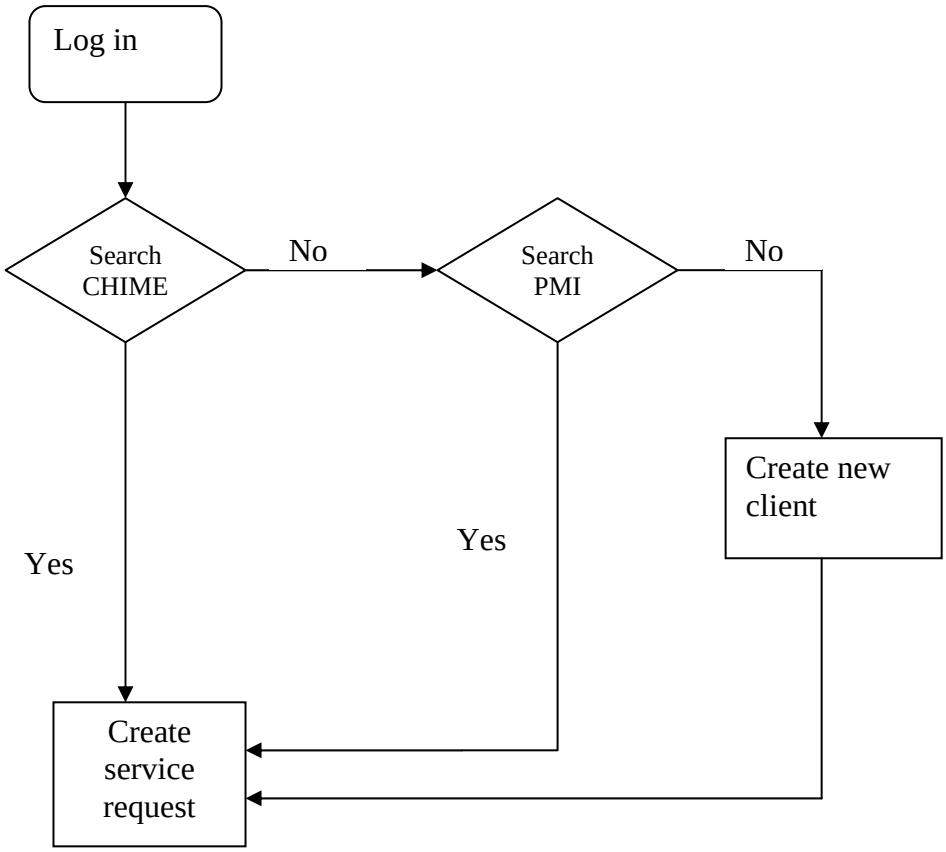

Figure. 7.2: Processes involved in CHIME

Possible failure mode of these processes are summarised in Tables 7.3 through 7.5.

Unable to log on to the system

1. System unavailable
   - 1.1. application failure
   - 1.2. hardware failure
     - 1.2.1. server problem
     - 1.2.2. desktop problem
   - 1.3. network failure
   - 1.4. power failure
2. Failed authorisation
   - 2.1. new user, no authorisation
   - 2.2. password failure
     - 2.2.1. incorrect password
     - 2.2.2. password expired

Table 7.3: Possible Failure modes for login

1. System unavailable
   - 1.1. application failure
   - 1.2. hardware failure
     - 1.2.1. server problem
     - 1.2.2. desktop problem
   - 1.3. network failure
   - 1.4.power failure
2. client's data unavailable
   - 2.1.data loss due to database failure
   - 2.2.file corruption

Table 7.4: Possible Failure modes for client search

1. PMI not available
   - 1.1. PMI server down

Table 7.5: Possible failure of search in Patient Medical Index

The initial password for Health Data Operating Centre is “PASSWORD”, hence there is a chance that another user logged in as the user with the latter’s access rights. The possibility of this occurrence was discussed with the CHIME Operations Manager and he stated that it could be possible, but he believed that the risk is not high as no one could gain advantage from it. Users need to change the initial password the first time they log on.

Potential failure mode: unauthorised user logged in with the initial password

Potential Causes: unauthorised user logged into the system

Severity: High

Probability: low

Hazard Score: 3

The user name for CHIME is fixed as surname and first initial. For example, the user name for John Smith will be smithj. Therefore, anyone can guess another’s username. As stated previously, unauthorised persons can log in with the initial password, “PASSWORD”. Therefore, if the data be available to unauthorised or unscrupulous users, and destruction or modification of data occurs, data can be lost permanently and can cause a detrimental effect on the patient. Therefore, the severity can be categorised as high. The probability can be categorised as low as this situation rarely or never occurs. Based on these, risk or hazard score can be categorised as 3 (refer to Table 7.2).

Potential failure mode: application failure

Potential Causes: system unavailable and client information could not be retrieved; creation of a new record; duplication of record

Severity: high

Probability: low

Hazard Score: 3

The chance of application failure is rare and the system administrator is available to assist clinicians with the application.

Potential failure mode: hardware failure

Potential Causes: system unavailable and client information could not be retrieved

Severity: high

Probability: medium

Hazard Score: 6

Potential failure mode: network failure

Potential Causes: system unavailable and client information could not be retrieved

Severity: high

Probability: low

Hazard Score: 3

Probability of network failure is low as the system is located within an Intranet and only authorised users use the system.

Potential failure mode: power failure

Potential Causes: system unavailable and client information could not be retrieved

Severity: high

Probability: low

Hazard Score: 3

If there is a power failure and if there is a no backup, it is difficult to trace back client information in fully computerised systems and the severity will be high. However, currently, since CHIME is a hybrid system supporting both paper - based and electronic formats, the severity would be low.

Passwords for computer logged on are set to expire after 40 days, and CHIME passwords expire after 60 days. The application will prompt 5 days ahead of the password expiry date. If the password is expired but has not been changed, the user would need to contact the CHIME system administrator.

Searches can be performed in CHIME and PMI (Patient Master Index) with surname or with Soundex. It is noted that there is a stronger match at the Soundex for PMI. Therefore, there is a need to improve the search algorithm used in CHIME. For example, if the last name 'Lightower' is spelled wrongly as 'Lightowler', it could not be found in CHIME, but the search function in PMI soundex could find the name.

Soundex was developed in 1800's to represent the phonetic similarity of names, e.g. Smith – S-530; Smyth – S-530. The soundex is a coded surname (last name) index based on the way a surname sounds rather than the way it is spelt. Surnames that sound the same, but are spelt differently (U.S National Archives and Record Administration 2000).

Duplicate runs are performed every month. In a newer version, - to be released in 2004 - the duplicate copy of the record will be only available as read only. The drawback is there may be an alert in the previous record for the client but it cannot be seen in the duplicate, and that could impact on the client.

Eligibility status to be cared/treated by community health is checked when the client first contacts the service. Initially, there would be a search to determine whether the client is already registered with the system. If the client's data is not available from CHIME, there will be a search for PMI from the server. Client search and PMI search could be performed as described in Figure 7.2.

Potential failure mode: data filled in another client's record

Potential Causes: client's name not displayed on every screen

Severity: high

Probability: high

Hazard Score: 9

That is the case in CHIME version 1, release 238 but this has been rectified and the patient's name will be displayed on every screen in the new release (CHIME version 1, 238-1).

Service request diary

Potential failure mode: Chance of wrongly selecting the different dates

Potential causes: wrong date for the appointment

Severity: high

Probability: low

Hazard Score: 3

When creating a service request, a 'crisis indicator' can be set according to the urgency to one of 20 levels – the default is 'not in crisis.'

Potential failure mode: wrongly setting the crisis level

Potential Causes: patients in a higher crisis level may be set to a lower level.

Severity: high

Probability: medium

Hazard Score: 6

There is no confirmation or summary of action – the latter would remind the user what selection they had made and would reduce possible errors from accidentally choosing the wrong selection.

Urgency

If it is an urgent case, the person needs to be attended to immediately.

Potential failure mode: wrong urgency level

Potential Causes: patient may not have an appointment according to the urgency level

Severity: high

Probability: medium

Hazard Score: 6

There is no confirmation or summary of which urgency level was chosen. There are different processes for urgent and non-urgent clients. According to the business process, the urgent client even has a different urgency level. If there is no fax regarding the patient information, the urgency level is set to 90 days and if there is a fax, the urgency is set to 14 days. Urgency level selection was discussed with the responsible person from CHIME. Although it is called urgency level, it was claimed that these cases are neither urgent nor emergency cases that need immediate care! However, it is the belief of this researcher that urgency level needs to be set according to the patient's level of attention.

Clinical notes can be documented in CHIME using either free-style or the inbuilt template. However if descriptions of current history of illness are in free style text, then it will be difficult to perform indexing or searching for future uses. In CHIME healthcare providers can also use a spell check if they wish. Therefore, the healthcare provider can still write clinical notes in abbreviated form and the spell check will not prompt for spelling changes.

In previous release of CHIME, the user could not know that there are images attached to the record, as there are no indications in the system; some scanned data may not be retrievable because of that. However, a newer release, (version 1, release 238-1), incorporates an icon showing there is an attached file in the record. However, if clinical notes are scanned in as an image, patient data may be in the record but will be difficult to data mine at some future time.

CHIME is not integrated with prescription/pharmacy systems or with laboratory results. Medication can be documented in CHIME with the drug generic name, frequency code and dosage. As discussed in Section 4.9.2, medication errors are one of the causes concerning patient safety and integrating these modules will have added value to CHIME.

Threats and vulnerability of the system

The following information was obtained in order to assess system vulnerability. The system is located in an Intranet which uses the IBM Citrix Server and ensures maximum security. There is both an external and internal firewall present in the system. The system monitors and captures traffic at any location within the network. Data files and databases are stored on the server. The database is centralised at the Health Department Operation Centre (HDOC), located in Liverpool; there is a mirror site –XDOC- at Homebush. Full backup of data is performed every 24 hours. A system log is performed every hour. Antivirus software is installed on all machines. The CHIME System administrator is available during normal office hours.

There is an authenticated login to the system. Each individual has their own password, guest/anonymous login is not allowed. The system provides password management functions to allow password changes to be effected.

User access level is predetermined, and user can access only according to their permissions. A list of users who can access the system is maintained. Access control is available for system usage and user responsibilities. There is a policy regarding access.

- Passwords can include combination of alphabetic, numeric and special characters

Potential failure mode: virus infection

There is anti-virus softwares installed on all servers, desktops and laptops but there is always the possibility of new viruses.

Potential Effect: file corrupted, data unavailable

Severity: high

Probability: low

Hazard Score: 3

Decision: As the severity is high, there should be action for the condition

Recommended Action: regular update of antivirus software

The virus attack can cause system downtime and could lead to data unavailability.

The system can be audited back for all transactions. Auditing of the data will be carried out by the Audit Department, however, currently, there is no auditing performed.

Confidentiality level for the system is as shown in Table 7.6.

None: Any other users can view service request **Partial**: any other user can view the service request label on the tree view but no details **Full**: Only the organization unit that created the service request can view the information.

Table 7.6: Confidentiality of the system

Security is controlled by the confidentiality level chosen during the service request wizard, and by the data sharing profile assigned by the System Administrator.

Table 7.7. lists the possible failure modes for CHIME.

Potential failure mode	Potential effect	Severity	Probability	Hazard Score
Virus infected	File corrupted, data unavailable	high	low	3
Log in with initial password	unauthorised user log into the system	high	low	3
Application failure	system unavailable and the client information could not be retrieved, creation of new record, duplication of record	high	Low	3
hardware failure	system unavailable and the client information could not be retrieved	high	medium	6
Network failure	System unavailable and the client information could not be retrieved	high	low	3
Power failure	System unavailable and the client information could not be retrieved	high	low	3
Client's name not displayed on every screen	Data filled in another client's record	high	high	9
Chance of wrongly selecting the different dates	Wrong date for the appointment	high	Low	3
wrongly setting the wrong crisis	Patient in higher crisis level may be set to the lower level.	high	medium	6
wrong urgency level as clicked wrongly	patient may not have an appointment according to the urgency level	high	medium	6

Table 7.7: Possible failure modes of CHIME

During the present study, user feedback was gathered through questionnaires which were distributed to the relevant healthcare providers using CHIME. Within the Illawarra Area Health Service (IAHS), CHIME has been started in 2 teams, - Aged Care Assessment Team (ACAT) and Illawara Child Development Centre (ICDC). Feedback from both healthcare provider groups was obtained and this is discussed in Section 6.2.1.

7.2.1. Feedback from healthcare providers

Out of 14 healthcare providers who corresponded, 6 stated that data entry is both at the point of care and also later from the paper based records. 7 correspondents stated that data is entered to the paper-based record system first, then entered

later to CHIME. One correspondent stated that dictated data is entered later into CHIME.

Availability of CHIME

Seven out of 14 healthcare providers stated they could connect to CHIME every time, but 6 of them stated there is a failure to connect to CHIME one to 3 times per month. 4 of the healthcare providers responded disagree with the ease of data retrieval.

Data can be easily retrieved from CHIME

a. strongly disagree	0
b. disagree	4
c. mildly agree	3
d. agree	6
e. strongly agree	1

6 of the 14 correspondents strongly agreed that duplications of records are often in CHIME. This needs to be rectified and search facilities of CHIME needs to be improved.

Duplication of records are often in CHIME

a. strongly disagree	0
b. disagree	6
c. mildly agree	5
d. agree	2
e. strongly agree	1

6 Respondents disagree that possible errors of data in CHIME is low.

5 out of 14 healthcare providers strongly disagreed that CHIME did not impede the workflow and 21 percent disagree that CHIME did not impede their workflow.

Data entry to CHIME did not impede the work flow.	
a. strongly disagree	5
b. disagree	3
c. mildly agree	3
d. agree	3
e. strongly agree	0

Table 7.8 and 7.9 include comments from users of the system.

- There are still a lot of bugs that have not been fixed up yet and are taking a long time working out. For example, adding service request to diary when there are more than one service requests.
- Unable to look up client details if in the middle of adding a new service request, keep having to exit and start again. Unable to go back into the comments/diagnosis box to add any extra details
- Unable to add referral directly from phone call, takes up too much time
- Comments box- limited space
- I spend much time away from where I have computer access to CHIME (That may change in future). Episodes of CHIME closing down when I am in the middle of data entry and losing all the information requiring data entry again.
- Have difficulty producing a monthly report that is brief and succinct with the relevant information. Will have to generate a paper report until this can be rectified.
- Most tasks take too many steps to accomplish. There is no ability to move backward and forward through multiple open windows with ease.
- Tasks and steps not done often are not easily relearned later and no reminder clues of the steps. Difficulty with multiple tasking, cut/paste etc.
- Time consuming, too many clicks, which may lead to muscle strain.
- Limited allowance of space for comments in issue screen
- Multiple service requests –fault in diary set up
- Simply takes more time each day
- We still need a paper file as well as CHIME. Diary isn't efficient.
- Some repetition/ duplication of information
- Some aspects of the system are clunky/time consuming
- Frustrating when the system is down and you cannot access client information
- Poor clinical notes editor, does not accept tables, no spell check etc.
- Still unable to get back to full case load
- Double handling of clinical note, written report then clinical note
- Diary is still very cumbersome for high throughput services
- Not being able to switch between screens when enquires are being made (losing data half entered)

Table 7.8: Problems encountered during using the system

- It is too easy to duplicate clients when no MRNs are present.
- Unable to go back into the comments/diagnosis box to add any extra details.
- Overall it is a good system but needs to upgrade particularly.
- Through 'PUAG' (Product User Advisory Group), we are making/seeing changes, but it is a slow process (due to time and resources)
- The screen for patient details e.g. Name, DOB, Address, Contact no., COB etc. would be easier if more detail on one screen
- Too many mouse clicks required to open "tree" for client- especially when they don't always work. Tree collapse if new data entered.
- Are we all recording our activities consistently?
- Looking forward to further implements.
- CHIME works very well- can see 'Big' Picture with its future.

Table 7.9: Comments regarding the system

7.2.2. Discussion on CHIME

The CHIME System administrator can browse all data. Data are not encrypted and that is of concern for information privacy, however all employees of the Illawarra Area Health Service need to follow a code of conduct and confidentiality. CHIME complies with the 12 principles of the Privacy and Personal Information Act of 1998 as well as the 15 principles of the Health Records and Information Privacy Act which comes into effect from September 1 2004.

According to the EHR Working Group's A NSW Health Strategy for the Electronic Health Record (EHR Working group 2001), benefits to consumers, providers and organization result through use of CHIME. Benefits to consumers include not having to provide the same information repeatedly and greater access to treatment plan information. Consumer/patient information can be accessed by authorised healthcare providers as CHIME is located within an Intranet. CHIME

has a common clinical interface with the public health system, for example systems from Wollongong Hospital. Therefore, healthcare providers can access treatment plan and information but in its current state, consumers do not have access to CHIME.

As CHIME has only been recently implemented in the Illawarra, it has not been able to fulfil all the benefits predicted by the NSW Health strategy for electronic health records. According to feedback from users, data entry is to the paper-based record at the point of care and entered into CHIME later. Therefore, currently it takes longer time and is not as efficient as forecast.

Users of the system also expressed concern about the system collapsing during the data entry, being unable to switch between screens during data entry, as well as data loss needing to be rectified as this is important for system reliability.

It is noted that the same PMI number system is used for both Illawarra community health and public hospitals in the Illawarra. Therefore, there is unique identification of patients in the public system, and moreover this information can be traced back. However, if the patient is from the private system, such as Figtree Private Hospital, there is no PMI number for the patient. Data from the private hospital and general practices would be connected through Health Connect as illustrated in Figure 6.4.

A patient's name and identification number are not displayed on every screen in the previous version of CHIME, and because of that data could be wrongly

entered into the wrong record, which can have a devastating effect on the patient. This has been fixed in the newer version of CHIME.

CHIME is located in an Intranet; connection is via a Citrix server, where there is a maximum security. CHIME users, system administrators, and all employees in IAHS need to comply with confidentiality and the code of ethics. A data confidentiality level is maintained in CHIME and there is also a data sharing profile.

Paper-based record systems still predominate in CHIME. Data is entered into paper based records and transferred to the CHIME later, thus it can be seen that the system is a Hybrid one, incorporating both paper-based and electronic health records. Therefore, there is duplication of work and the possibility of not entering all data in CHIME.

As CHIME caters for 39 programs, the application is not specifically designed for each discipline. Therefore, it can be seen that there are no specific fields or subsystems such as cardiac, respiratory etc. to Service Contact details. Warren et. al (2003) identified that “clinicians differ in specialty, experience, practice context, practice style”. Different specialties need different data set for healthcare delivery; it would be impossible to incorporate all different data sets in one system and incorporating only essential data would also not provide all the needs of clinicians. CHIME uses its standard architecture to cater for all these programs instead of using a federated system approach. Therefore, there are some workflow problems as described in Table 7.8 and 7.9.

In CHIME, deleted text still appears and as a line striking through the error, which is an important safety feature for medico-legal purposes.

7.3. Risk assessment case study – MINET (Simpson Centre for Healthcare Innovative Research)

This case study was conducted at the Simpson Centre for Healthcare Innovative Research using the Maternal and Infant Network (MINET) database. MINET is an appropriate case study for this research as it involves different electronic health data from several different sources.

7.3.1. System description

The MINET database contains health data on infants and children in the South Western Sydney Area Health Service from the prenatal period to school age (0 – 5 years). MINET involves Community Based Data from the Ingleburn Baby Information System (IBIS Database) and the Obstetric and Gynaecology Data (OBSTET). IBIS is used by all five sectors of the South Western Sydney Area Health Service. The system collects information from each of these sectors regarding well baby clinic visits. The IBIS database holds baseline data on 10,000 babies and their mothers and 50,000 visits to health services by these infants and their mothers. There are more than 4,000,000 data items on the database.

Data in these databases are important for public health and health service research. The database supports evaluation of services, review and re-configuration of services where necessary to achieve specified improvements in outcomes or to better access for people with identified risk (Phung et. al. 2004). These data are important because prenatal, infant and early childhood periods are critical for the promotion of good health and the development of the personal characteristics for adolescence and adulthood (Halldorsson et al. 1999). Therefore, it is important that data in these databases are accurate and free from errors for various purposes for health service research.

OBSTET data are downloaded to the SIMPSON Centre for health research purposes only, however the SIMPSON Centre does not have any control over how this data is collected and processed. OBSTET data are downloaded as .CVS files and uploaded into Microsoft Access databases for comparison and linking for research purposes.

Currently, IBIS Version 4 is being used in the SWSAHS. IBIS uses Optical Mark Recognition (OMR) to capture data. IBIS is part of a Local Area Network, which enables sharing of information with other service points for mothers and their babies.

There are two types of data within IBIS; baseline and follow-up. The IBIS baseline form is used for the first visit and the IBIS follow up form for follow up visits. An IBIS baseline data form and IBIS follow up forms are included in Appendix A.

Processes involved in MINET database are described in Figure 7.3.

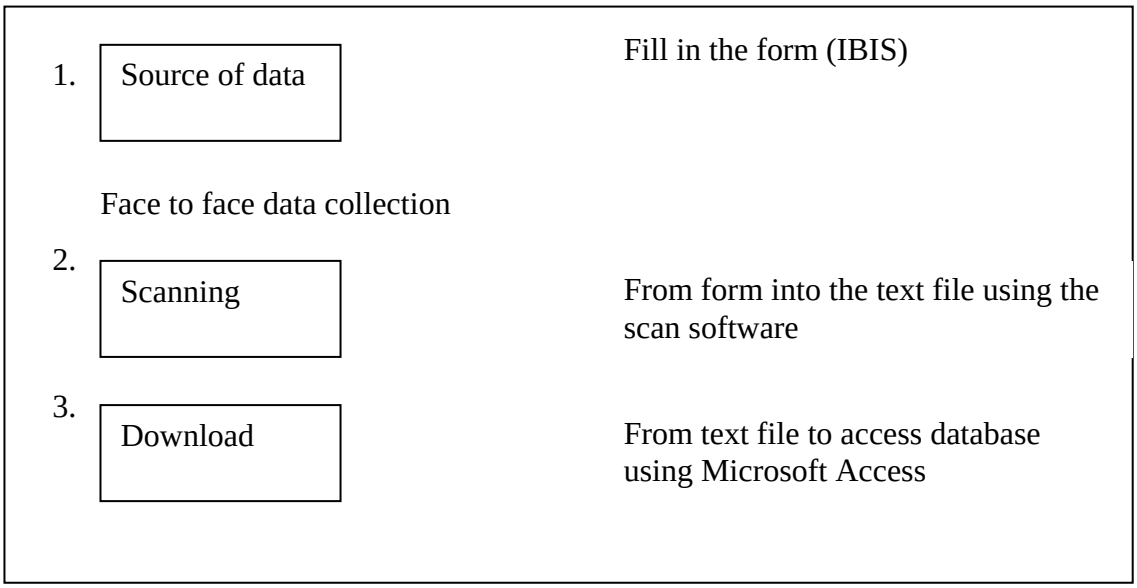

Figure 7.3: Processes involved in MINET database

Possible Failure Mode from these processes are summarised in Figure 7.4.

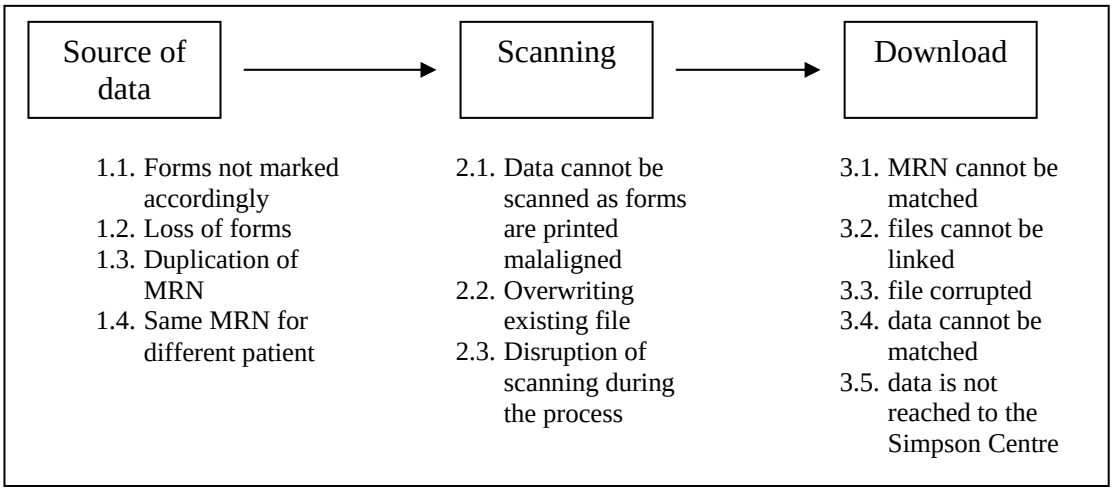

Figure 7.4. Possible failure modes from processes

1.1. Potential failure mode: Forms are not marked accordingly

Potential effect: incomplete data

Severity: high

Probability: medium

Hazard Score: 6

The level of risk is intolerable as inaccurate or incomplete data can impact on the research data. Forms that are not marked accordingly need to be ruled out at the time of scanning. This can be due to human error and the Simpson Centre needs to trace them back to the relevant community health unit.

1.2. Potential failure mode: Missing forms

Potential effect: incomplete data

Severity: high

Probability: medium

Hazard Score: 6

Patient data are filled in manually at the community health centres and compiled prior to scanning. Scanning is performed in batch processing. Some documents can be misplaced and lost at the time of scanning. This is intolerable as incomplete data can have an impact on health service research, predicting high risk cases and impact on healthcare indicators. To counteract this problem - "Missing forms"- it is advisable to have computerised data entry at the point of care.

1.3. Potential failure mode: different Medical Record Number (MRN) for the same person

Potential effect: data unavailable or misleading data

Severity: medium

Probability: medium

Hazard Score: 4

The same patient may visit different area health services and there can be different MRNs for the same person. Therefore, there can be incomplete data or duplication of data. The risk should be classified as ALARP which is not regarded as negligible but something that should be under review in order to reduce it further.

1.4. Potential failure mode: same MRNs for different patients

Potential effect: misleading data for research purposes

Severity: high

Probability: medium

Hazard Score: 6

Data may be linked to the wrong patient at the time of analysis and there can be errors in focusing health indicators, it is an intolerable risk. Correctly identifying the patient is very important and implementation of unique patient identifiers will improve this situation in the future.

2.1. Potential failure mode: forms are printed misaligned

Potential effect: documents unscannable

Severity: low

Probability: low

Hazard Score: 1

The probability of unscannable documents is low; forms are outsourced to professionals and they are designed to make sure that are well aligned.

2.2. Potential failure mode: overwriting an existing file

Potential effect: data loss

Severity: high

Probability: low

Hazard Score: 3

Files need to be saved after scanning. If they are overwritten, there can be possibility of data loss. The level of risk is unacceptable. To prevent this, there is a naming system in place. There is a step-by-step procedure for saving files, confirming and checking before saving and that could prevent overwriting. This hazard has been addressed in the MINET user manual.

2.3. Potential failure mode: disruption during the scanning process

Potential effect: incomplete data entry

Severity: low

Probability: medium

Hazard Score: 2

There can be disruption during the scanning process, which can be due to mechanical problems with the machine, power failure or due to the inexperienced operator. Such disruption can be detected during the scanning process and the problem can be fixed so that it would not have a significant impact on the system. There will be only impact on the scanning job at the time and would need to repeat the process. The risk has therefore been identified as acceptable.

3.1. Potential failure mode: MRN cannot be matched

Potential effect: maternal and infant linked wrongly

Severity: high

Probability: medium

Hazard Score: 6

It is noted that different medical record numbers (MRNs) are used in different services; maternal MRN and infant MRN are different. There is a possibility of wrong association of maternal and infant MRNs. The likelihood is higher when the mother's surname and child's name are different. It was noted that this probability of occurrence is about 20-30%. For example, a mother from a different ethnic origin may not change her surname after marriage, with the result that the mother's surname and the infant surname may be different. If the parents are not married, the surnames will be different. Sometimes, a mother's surname was changed from the previous childbirth history as a result of marriage or divorce. Therefore, there can be duplication of MRNs for the same person at different services or at the same service. The level of risk is unacceptable.

3.2. Potential failure mode: files cannot be linked

Potential effect: data unavailable for research purposes

Severity: high

Probability: low

Hazard Score: 3

Files cannot be linked if the system is unavailable. There can be different causes for system unavailability, including power loss and application failure. The

Simpson Centre has yet to experience application failure. However, as the system is not a real time one, power loss for a certain period is also acceptable.

3.3. Potential failure mode: file corrupted

Potential effect: data unavailable

Severity: high

Probability: low

Hazard Score: 3

There will be loss of data if the data file is corrupted. The Simpson Centre has regular backup of data in order to prevent this.

3.4. Potential failure mode: data cannot be matched

Potential effect: impact in analysis of data

Severity: high

Probability: high

Hazard Score: 9

3.5. Potential failure mode: data has not reached to the Simpson Centre

Potential effect: impact in analysis of data

Severity: high

Probability: low

Hazard Score: 3

Data collected from Community Health in paper form has been misplaced - probability is low. This could be prevented by direct data entry to the computerised system.

Threats and vulnerability of the system

To assess MINET information security and vulnerability to threats, information regarding the system was obtained. It is noted that the system is located on the Local Area Network. Anti-virus software was installed on all servers, desktop and laptops. There are Firewalls, both internal and external, to protect information. There is an audit trail configured to log all transactions. Log file analysis is carried out daily and reports of unusual/inappropriate/anomalous activities are sent to the system administrator for necessary action. The system ensures the prevention of unscrupulous system attacks.

MINET ensures confidentiality and privacy of the health data. Each patient has consented to disclose the information for research purposes. There is an authenticated log in to the system. There is a policy regarding the access. There is a list of users who have access to the system. User access level is predetermined and users can access only according to permissions. Access control is available for system usage and user responsibilities. There is a user group for MINET which determines access levels.

The system provides a password management function to allow password changes to be announced. Account authentication cannot be eavesdropped. Each individual has their own password. Guest/anonymous login is not allowed in case

of breach of confidentiality, as it is difficult to trace back. Passwords include a combination of alphabetic, numeric and special characters. A first time password is transmitted securely.

The system is a distributed system and data files and database are stored on the server. The back up is performed at the Simpson Centre and the other community health service centres. Back ups are stored securely under lock and key. The Information Service Department has back up of data on tapes and the Simpson Centre has a data back up on hard disks.

The Simpson Centre uses de-identified data for research purposes and maintains patient confidentiality. The Centre follows the 'Database and data extracts policy and guidelines' of the South Western Sydney Area Health Service.

4.1.Potential failure mode: the system is attacked by the intruder

Potential effect: breach of confidentiality

Severity: High

Probability: low

Hazard Score: 3

System vulnerability was tested. The system is in Local Area Network with no access from outsiders.

4.2. Potential failure mode: Staff member stolen the patient information

Potential effect: breach of confidentiality

Severity: High

Probability: low

Hazard Score: 3

The level of access to the system is predetermined. Staff members can access the data but the threat is unlikely as all staff members need to follow the privacy and confidentiality guidelines.

Table 6.10 lists all potential hazards, together with their frequency of occurrence and severity.

Potential failure mode:	Potential effect	Severity	Probability	Hazard Score
1.1. Forms are not marked appropriately	incomplete data	high	medium	6
1.2. Forms missing	incomplete data	high	medium	6
1.3. Different MRNs for the same person	data unavailable or misleading data for the research purpose	medium	medium	4
1.4. Same MRN for different patients	misleading data for the research purpose	high	medium	6
2.1 .Forms are printed malaligned	Documents unscannable	Low	Low	1
2.2. Overwriting an existing file	Data loss	High	Low	3
2.3. Disruption of the scanning process	Incomplete data entry	Low	Medium	2
3.1. MRN cannot be matched	Mother and infant linked wrongly	high	Medium	6
3.2. Files cannot be linked	Data unavailable for research purpose	High	Low	3
3.3. File corrupted	Data unavailable	High	Low	3
3.4. Data cannot be matched	Impact in analysis of data	High	High	9
3.5. data has not reached the Simpson Centre	Impact in analysis of data	High	low	3
4.1.The system is attacked by the intruder	Breach of confidentiality	High	Low	3
4.2. Staff member stolen the patient information	Breach of confidentiality	High	Low	3

Table 7.10: Possible failure modes for MINET

There is a high probability that data cannot be matched properly as different versions of IBIS have different data units. These need to be fixed at the time of form download.

Wrong linkage of data can lead to incomplete or inaccurate data. This can have a great and immediate impact on patients, assuming this relates to the clinical data. The Simpson Centre uses aggregated data for statistical analysis and records that are not perfectly matched are excluded from the analysis. Exclusion of records will lead to change in data and this can change the percentage of health outcome or health indicators as all data cannot be included in statistical analysis.

The Simpson Centre uses de-identified data for research purposes and maintains patient confidentiality. The Centre follows the 'Database and data extracts policy and guidelines' of the South Western Sydney Area Health Service.

The Simpson Centre uses data mainly for health service research. Health services research is important as it could effectively improve the public health. Health service research can focus on the healthcare processes, disease pattern, disease surveillance, prevention of disease and promotion of health. The Simpson Centre IBIS data are uploaded to the system via batch processing. If the data is real time, it can be useful for surveillance of disease outbreak or bioterrorism.

The focus of the Simpson Centre MINET database is on maternal and child health. The IBIS manual clearly explains the format of questions, why the data is collected, what the data is about and standard for completion. It is noted that

IBIS data has been considered for data completeness, legibility and integrity of information. Data are gathered with a clear understanding of what they would be used for in the future. This is very important as there can be errors in interpretation and outcome if the purpose is not clearly specified (Warren et. al 2003; Shortliffe and Barnett 2001). There is a clear explanation of privacy policy and those involved with data entry and/or, data processing also are aware of the confidentiality. Access level is decided by the user group and the administrator needs to set the access level accordingly and ensure data privacy.

As data from different databases are used for research, common data standards are important for different databases. Inaccurate or incomplete information can have an impact on both research and disease surveillance. Completeness of data is essential for MINET databases, as incomplete data will result in statistical analysis error, which will impact on healthcare indicators.

7. 4. Chapter Summary

It is noted that as in the literature, different electronic health record systems are in use in different health care organizations. Although NSW has targeted to implement a full electronic health record system by 2010, it can be seen that a hybrid approach (both paper and electronic) is still predominant in the health record system case studies conducted as part of this study (CHIME and MINET). Based on probable near miss events these systems have been modified accordingly.

While CHIME has been in use in the Illawarra for less than two years now and although users have received the appropriate training, the system is not yet mature and users are still in a period of transition. During the course of this study, it was found that to date users are not confident enough to use the system, and moreover believe that it impedes their workflow.

CHIME electronic health records fulfil the primary purpose of electronic health records categorised by Scholeffel and Jelson, as CHIME constitute a documented record of care by means of communication among clinician's, thereby contributing to the patient's care. According to EPR (Electronic Patient Record) levels identified by NHS UK (discussed in Chapter 2) CHIME can be categorised as a level 2 EPR.

CHIME has diverse groups of stakeholders such as the Commonwealth Department of Health and Aged Care, New South Wales Health, Community Health, Illawarra Area Health Service, clinicians, nurses, and administrators. It also caters for different community health services; it is not customised for specific user groups.

The main Stakeholder of MINET is the Simpson Centre. The system is implemented for a specific purpose and is customised according to the needs of the Simpson Centre – namely health services research.

It can be seen that implementation is a process of modifying the system continuously and both CHIME and MINET have been modified subsequently to

adapt to the needs of users. Potential system risks, such as misidentification of patients, security breaches due to initial password, and incorrect linkage of data were identified and notified to the appropriate personnel. Improvements to both systems have been achieved through system modification based on the results discovered from the case studies.

Both MINET and CHIME are based on community health data focusing on different information management. However, both systems need to have unique patient identification to decrease duplication of records for better information management. Also the search function in CHIME needs to be improved so that longitudinal healthcare data will be available for patients.

Both systems are hybrid ones, with information also stored in paper-based form. Data for the Simpson Centre needs to be filled using templates which are scanned in later. There could still be problems of loss of records before scanning; computerising the record systems could solve this problem. However, as the data collection is conducted in different locations, there is a need for infrastructure, which is currently impossible to implement because of resource limitations.

As discussed earlier, in CHIME the notes or observations from clinical encounters need to be filled in as free text format, and there is no structure for health care episodes. If the data were in a structured format, it would be easier for data entry, retrieval, and search. In CHIME, users need to move from one screen to another to fill in data, appointments, service requests, and so on, which is time consuming. This highlights that the system needs to be easy to use. User

of the system also pointed out in the feedback that the system is not easy to learn and is impeding the workflow. Impeding clinician's workflow will have an impact on the safety and quality of healthcare.

Therefore, the *system* quality attributes-such as ease of use, response time and usability of the data are as important as the *data* quality attributes for the safety of the electronic health record systems and they should be included in any safety assessment of electronic health record systems.

It is noted that users consider an 80 percent match of an integrated record as being 'highly matched' from the perspective of legacy databases integration. Users would not use the data to analyse health status or for healthcare research if they are not fully matched, but a matching algorithm needs to be improved for safety. The following description illustrates what 99.9 percent means for data

Please see print copy for Table 7.11

Table 7.11: what 99.9% means (http://www.npsf.org/listserv)

Therefore, perfect match of data is very important and data should be linked perfectly. User awareness and understanding of safety is very important for building safer health systems.

Safety attributes of electronic health record systems have been identified in Chapter 4. Empirical studies from CHIME and the Simpson Centre described in this chapter proved that these attributes (Table 4.9) are essential.

The importance of uniquely identifying patients could be seen from both case studies. Problems and possible effects from having duplicate records or patients not being able to be identified were discussed in the CHIME case study. Potential near miss events have been identified and the newer version of CHIME will have the patient's name and identification displayed on *every* screen. MINET uses data for research purposes and uses aggregated data. Therefore, a patient's name and identification on every screen is not applicable to the MINET data. However, there were lots of problems in linking data as patients could not be uniquely identified,-for example, duplication of MRN, same MRN for different patients, different MRN for same patients, impossible to link the mother and the baby and so on. These supported the contention that unique identification of patients is very important for patient safety.

Both MINET and the CHIME ensure privacy and confidentiality of data. Neither systems, is directly connected to the Internet and thus attacks from the outside world are prevented. To prevent attacks from email attachments and intrusions, internal and external firewalls are present in both systems; antivirus software is

also installed. However, there was no data encryption in either system. Details of authorization and access levels of CHIME and MINET were discussed in Sections 6.2 and 6.3. Patient consent was taken in paper-based form in both systems. There is a policy regarding access to data. User access level is predetermined and user can access only according to their associated permissions.

Neither system is integrated with the physician order entry system or pharmacy databases. Based on this study, it is recommended that CHIME should incorporate or integrate with medication management system.

Results on case studies demonstrated that safety attributes identified for EHRs in Chapter 4 are appropriate for EHRs. Table 7.12 demonstrated the relationship between the results from the case studies and the safety attributes.

Attributes	Case studies	discussed
Identification	Near miss incident in CHIME and impact of wrong linkage of data due to patient not identified uniquely in MINET	✓
System security	Both case studies highlighted the importance of system security	✓
Privacy	Both case studies highlighted the importance of health information privacy, and discussed the importance and prevention of privacy breaches.	✓
Confidentiality	was highlighted in both case studies	✓
Consent	was involved in both studies.	✓
Disaster recovery	To ensure accuracy and availability of data in both studies (claimed by both organisations)	✓
storage	To ensure data quality in both studies	✓
Backup	It was discussed in both studies regarding importance of back up and the data loss	✓
Retention period	It was to have the historical data for the MINET database(claimed by both organisations)	✓
Data standards	discussed in both studies - enhances data interpretability and the relevance	✓
Data interoperability	was discussed in both studies	✓
Data integrity	was highlighted in both studies	✓
Medication	The MINET database needs to include the history of medication for research purposes. It was suggested to CHIME for error prevention in medication	✓
Alerts	It was suggested by the author to include different alerts for CHIME for safety purposes (but no action taken at this stage)	✓
Data entry	The importance of accuracy in data entry was discussed in both studies	✓
Attributes of data quality	Data quality attributes were reviewed in both studies to ensure safety	✓
System quality	Importance of usability, accessibility and ease of use were highlighted in both case studies.	✓

Table 7.12: Relationship of identified safety attributes and case study results

Awareness of safety is very important for an organization. Healthcare organisations need to accept that there could be different risks to their system. During this study the author has noted that some aspects of questions are

sensitive for the organisation and interviewees would prefer to claim that the system exhibits minimum risk only and that all aspects are covered. The safety culture of an organisation is important and reporting adverse incidents should not be taken as a reason to blame or litigate. Therefore, a culture, where acknowledgement of error is not acceptable (Nieva and Sorra 2003) should be changed in health care organisations and reporting incidents and identifying errors should be seen as a positive move towards building the safer health care systems.

There needs to be collaboration and understanding among the administration, technical staff and healthcare providers as the latter need to use the system for different purposes. Thus feedback from users should be considered as input for system improvement and not as negative criticism. However, aspects of social and organisational behaviours are beyond the scope of this research.

Risks associated with electronic health records can have an impact on diagnosis, treatment and preventive care. When designing EHR systems, it is important to decide how safe is 'safe enough', without under-designing or over-designing the system. Whenever a new system is implemented or changes affected within it, time is needed for users to adopt and adjust. Especially in EHR systems, where there is reluctance to use the system, system developers should assist and increase efficiency and workflow. Including safety measures should hinder neither the adoption nor use of EHR systems.

This study also demonstrated that a federated system approach would be preferable to a standard EHR architecture. Problems encountered from CHIME users clearly demonstrate that the system is not tailored to specific user needs and instead tries to incorporate all different programs. In CHIME, users need to adapt to the system; and the system does not tailor to the clinicians needs.

In conclusion, this study has identified an appropriate risk assessment method of the electronic health record systems conducted safety assessment of the electronic health record system and highlighted the role of electronic health record systems in building safer health systems.

CHAPTER EIGHT

Conclusion and Recommendations

In this concluding chapter, a summary of the key findings of this dissertations are presented. This research has identified a relationship between dependability and data quality of EHRs and attributes for safety assessment. The research involved (i) developing a theoretical basis of safety, based on dependability and data quality, (ii) defining the safety attributes of EHRs, (iii) identifying a risk assessment method applicable to EHRs, and (iv) conducting EHR case studies in different healthcare settings. Answers to the research questions were also realised.

8.1. Summary of research findings

The research questions posed in Chapter 1 were, “How can the safety of EHRs be measured?” and “what are the safety attributes of EHRs?” The safety attributes of EHRs were identified from this study and described in Section 4.12. Results from the empirical case studies reinforced that the safety attributes previously identified are appropriate for EHRs. Chapter 5 identified the appropriate risk assessment method for EHRs and answered the research question, “how can the safety of EHRs be measured?” The following section documents the research carried out and demonstrates that the research aims have been met. The general research aims were:

i. To demonstrate that EHRs need to be dependable

The importance of dependability of EHRs was discussed in Chapter 4, including detailed case examples for EHRs. The empirical case studies of MINET and CHIME clearly demonstrate that of dependability attributes: - availability, reliability, safety and security - are critical for the EHRs.

ii. To identify the appropriate risk assessment method applicable to EHR Systems

This research has identified that risk assessment methods traditionally used in other industries can be applicable to the safety and risk assessment of EHRs. These risk assessment methods applicable to EHRs were thoroughly discussed in Chapter 5. Failure Mode Effect Analysis (FMEA) was identified as the appropriate risk assessment method for EHRs as this risk assessment method is a proactive risk assessment. It is important to identify and prevent potential failures before happening. With FMEA, possible failure modes involved in all the processes can be identified and recommended the necessary action to prevent adverse events. Risk assessment case studies conducted on CHIME in the Illawarra Area Health Service and MINET in the Simpson Centre (SWSAHS) verify that FMEA is indeed the appropriate risk assessment method for the EHRs.

iii. To demonstrate that EHR systems are safety related system

Sections 4.9 and 5.2 discussed and established that EHRs are safety- related systems; this was also supported by the findings from the case studies discussed in Chapter 6.

Safety systems are systems whose failure may result in injury or loss of life (Sommerville 2001). Data in EHRs could be essential in healthcare decision making process and an error or inaccurate information can impact in healthcare process. This could have undesirable outcomes on patient's health and may even endangering patient's life. Potential near miss events, potential harm events and dangerous situations have been identified in both case studies, for example, potential near miss events in CHIME from not being able to uniquely identify the patient.

iv. To identify the risks associated with EHRs by evaluating safety, privacy and availability of such systems

This has been established by way of the empirical CHIME and MINET studies. Potential risks of CHIME and MINET were identified in tables 6.7 and 6.12 respectively. These include potential risks such as system unavailability, incomplete data entry, breach of confidentiality, data loss, impact on data analysis and so on.

Research findings from the empirical studies indicated that the research questions have been answered. Sections 6.2. and 6.3 described in detail risk assessment case studies conducted in CHIME, Illawarra and MINET Simpson Centre respectively. The case studies supported that the safety attributes identified in Chapter 4 are appropriate for EHRs and that FMEA is a suitable method for risk assessment of EHRs. The importance of uniquely identifying patients was discussed in both case studies. The importance of data entry, verification and

validation were also highlighted in both case studies. Data interoperability and data linkages with other systems are essential in both systems. These studies also highlighted the significance of data quality attributes such as availability, accuracy and completeness. Privacy, confidentiality and security of systems are essential in both systems, and there are appropriate principles, policies and systems in place in both CHIME and MINET. Both studies demonstrated the dependability attributes: - availability; reliability; safety and security - are important for patient safety. The case studies also highlighted that system quality attributes such as ease of use and usability should also be included in the safety attributes of EHRs.

To sum up, the key original contributions made by this dissertation are summarised in Table 8.1

SUMMARY
10. identification of the appropriate risk assessment method for EHRs
11. identification of the safety attributes of EHRs
12. outlining the relationship framework for dependability and data quality of EHRs
13. identification of factors which need to be considered in EHR risk assessment
14. EHR Risk assessment case studies of 2 healthcare organisations
15. Recommendations for modifications and changes to EHRs based on results obtained from these case studies

Table 8.1. Original contributions made by this dissertation

In conclusion, this research has identified the appropriate risk assessment method for electronic health record systems and identified safety attributes essential to EHRs. As purposes, functionalities and processes can vary from one EHR to another, any risk assessment needs to be tailored to the specific needs of the EHR concerned. By focusing on EHR risk assessment, this study has addressed some of the issues and challenges concerning the safety and quality of healthcare, thereby contribution to the building a safer health system(Kohn et al 2000).

8.2. Recommendations for future research

Improving patient safety in healthcare is a pertinent concern for today's healthcare industry. As a result of the risk assessment of the EHR systems further research questions for future research could include:

- Research of healthcare culture on safety

As the data included in EHRs are patient sensitive health information, only the test data and training system can be used for the purpose of risk assessment in this study. This research focused on the failure of technology and not on the human failures. Organisational culture and behaviour also impact on system failure. However, these are beyond the scope of this research. As it can be seen from current research, the culture of healthcare plays an important role in system safety. Identifying and reporting errors should not be treated as reasons for blame but should be considered as striving towards improving safety. Awareness of

safety in healthcare organisation is very important. Analysing the organisational culture will have a beneficial effect on the prevention of medical errors. Therefore researching the following areas will be beneficial to the safety of the healthcare organisation:

1. Organisational behaviour and culture of clinical incident reporting, and
2. Research into how to promote clinical incident reporting without blaming.

- Socio-technical probabilistic risk assessment

Risk assessment of EHR systems was undertaken in this research. Active and latent failures (discussed in Chapter 4) are caused by human, organisational and technical failures. As these are all interrelated, analysing socio-technical probabilistic risk assessments would be beneficial from the viewpoint of healthcare system safety. Therefore extending the probabilistic risk assessment method conducted in this research to the socio-technical probabilistic risk assessment would be beneficial.

- Consumer involvement in improving patient safety

Consumer health informatics is important for patient safety. Information stored in EHRs is of consumer health information and if this information could be available to consumers/patients, people could take greater responsibility for their healthcare. As discussed in Chapter 4, consumers need to know where their information is stored, for what purpose and who can access this information. Consumer feedback is also important for adverse drug reactions (O'Brien and

Yearwood 2003). Health information available to consumers is important as it would encourage consumers to be active partners in their healthcare. Consumers receive their healthcare from different healthcare providers, thus granting consumer access to EHRs would enhance consumers to be full partners in managing their own health. Implementing web-based Personal Health Records would enhance consumer involvement in healthcare and play an important role in patient safety. Therefore, research of consumer involvement in healthcare, availability of health information to consumers, the current state of personal health record systems, and the role of consumers in enhancing safety would all add value in improving patient safety.

- Mobile data devices

Patients may consult different healthcare providers throughout their life, likewise healthcare providers may need to visit patients for different purposes - for example, ambulatory care provider, making home visit, doctors visiting patient at their bed site, ward rounds in hospitals. Therefore, it can be seen that healthcare is mobile and integrating mobile data processing would be beneficial to healthcare. Therefore, studying whether wireless technology will have added value to healthcare safety would be an important area of research to investigate.

Patient safety is an important issue in the healthcare industry. This research identified the appropriate safety assessment for the EHRs, outlining the relationship framework for dependability and quality of EHRs. It can be seen that data in EHRs reflect the process and outcome of healthcare delivery and conducting risk assessment of EHRs can indeed enhance the quality and safety of

healthcare. Therefore, identifying the appropriate risk assessment for EHRs is indeed a valuable asset for health informatics.

BIBLIOGRAPHY

AHIMA Data Quality Task Force (1998), Data Quality Management Model, Journal of AHIMA, June, http://www.ahima.org/journal/pb/98.06.html

Academy for Health Services Research and Health Policy (AHSRHP), 2001, Glossary of terms commonly used in healthcare, available at: http://academyhealth.org/publications/glossary-healthcare.htm

Aikins R. (2000), Risk management methodology for HIPAA security standard. Journal of Healthcare Information Management, vol; 14(4), pp 29-40.

Amatayakul M. (1998), The state of the computer based patient record, Journal of American Health Information Management Association, October, http://www.ahima.org/journal/features/feature9810.1.html accessed February 2001

American Academy of Pediatrics: Pediatric Practice Action Group and Task Force on Medical Informatics(1999), Privacy protection of health information: Patient rights and pediatrician responsibilities, vol. 104 pp 973-977

American Health Information Management Association (2001), Standards for privacy of individually identifiable health information: A brief summary of the final rule, http://www.ahima/final_rule_summary.html accessed March 2001

AMIA 2005, Got EHR, available at http://www.amia.org/gotehr/info.html

Ammenworth E, Buchauer A., Bludau B, Haux R. (2000), Mobile information and communication tools in the hospital, International Journal of Medical Informatics, vol. 57, pp

Anderson R. J. (1999), Information technology in medical practice: safety and privacy lessons from the United Kingdom, The medical journal of Australia, Feb 15, vol. 170, is 14, pp 181-185

Appavu S. I. 1997, Analysis of unique patient identifier option: final report, United States Department of Health and Human Services, available at http://www.ncvhs.hhs.gov/app11.htm accessed August 2004

Arts D. G. T., Keizer N. F.D, Scheffer G-J., (2002), Defining and improving data quality in medical registries: A literature review, case study, and generic framework, Journal of American Medical Informatics Association, vol. 9, 600-611

AS/NZS 4360:2004 (2004), Risk Management, Standard Australia

AS/NZS 3931:1998, Risk Analysis of Technological Systems- Application Guide, Standard Australia

AS 4937-2002 Australian Standard (2002), Electronic messages for exchange of claim and related information, Standards Australia, ISBN 0 7337 4247 5 www.standards.com.au, accessed on 29 May 2002

AS ISO 15489- 2002 Australian Standard (2002), Records Management, Standards Australia, ISBN 0 7337 4346 3 www.standards.com.au accessed on 29 May 2002

ASTM, http://www.astm.org

Ash J. S., Bates D. W. (2005), Factors and forces affecting EHR System Adoption: Report of a 2004 ACMI Discussion, Journal of American Medical Informatics Association, vol. 12, pp. 8-12

Ash J. S., Gorman P. N., Seshadri V., and. Hersh W. R., Computerized Physician Order Entry in U.S. Hospitals: Results of a 2002 Survey, Journal of American Medical Informatics Association, PrePrint published November 21, 2003; doi:10.1197/jamia.M1427

Ash J.S., Gorman P.N., Lavelle M., Payne T.H., Massaro T.A., Frantz G.L., Lyman J.A., (2003), A cross-site qualitative study of physician order entry, Journal of American Medical Informatics Association, vol.10, pp. 188-200

Australia's Health 2002 (2002), The eight biennial health report of the Australian Institute of Health and Welfare, Australian Institute of Health and Welfare, Canberra, AIHW, Aug 2002, ISBN 174024 191 6

Bates D.W., O'Neil A.C., Boyle D., Teich J., Chertow G.M., Komaroff A. L., Brennan T. A. (1994), Potential identifiability and preventability of adverse events using information systems, Journal of American Medical Informatics Association, vol. 1, is. 5., pp 404- 411

Bates D. W., Cohen M., Leape L.C., Overhage M., Shabet M. M, Sheridan T. (2001), Reducing the frequency of errors in medicine using information technology, Journal of American Medical Informatics Association, vol. 8, no. 4, pp. 299-308

Bates D. W., Ebell M., Gotlieb E., Zapp J., Mullins H. C. (2003), A proposal for electronic medical records in U.S. primary care, Journal of American Medical Informatics Association, vol 10, is. 1, pp 1-9

Battles J. B., Lilford R. J. (2003), Organizing patient safety research to identify risks and hazards, Quality and Safety in Health Care, vol:12, pp ii2-7

Bakker A. R. and Leguit F. A. (1999), Evolution of an integrated HIS in the Netherlands, International Journal of Medical Informatics, vol.54, pp.209-224

Bakken S, Campbell K. E, Cimino J. J, Huff S. M, Hammond W. E. (2000), Toward vocabulary domain specifications for health level 7 – coded data elements, Journal of American Medical Informatics Association, vol.7, pp 333-342

Beale T. (2001), Health Information Standards Manifesto, revision 2.5, available at http://www.deepthought.com.au/health/HIS_manifesto/his_manifesto.pdf accessed May 2002

Berman J. (2003), Patient Smart Cards Gain in Popularity, Self Use, Health-IT World, available at http://www.imakenews.com/health-itworld/e_article000185703.cfm accessed January 2004

Blackhurst D. (2003), Hospital pays out £ 3.1 million for medical blunders, available at http://www.nhsexposed.com/patients/hospitals/nstaffs/blunders.shtml

BMA ethics (2001), http://web.bma.org.uk/public/ethics.nsf/webguidelinesvw?openview accessed May 2001

Board of Directors of the American Medical Informatics Association (1994), Standards for medical identifiers, codes and messages needed to create an efficient computer-stored medical record, Journal of American Medical Informatics Association, vol. 1, is. 1, pp 1-7

Booth N. (2003), Sharing patient information electronically throughout the NHS, British Medical Journal, Jul 2003, vol. 327, pp 114-115

Bouma G. D. (1996), The research process, third edition, Oxford University Press

Boynton P.M., Greenhalgh T. (2004), Hands on guide to questionnaire research: selecting, designing, and developing your questionnaire, British Medical Journal, vol. 328, pp 1312-1315

Brunner H.H., Conen D., Günter P., von Gunten M., Huber F., Kehrer B., Komorowski A., Langenegger M., Scheidegger D., Schneider R., Suter P., Vincent C., Weber O. (2001), towards a safe healthcare system: Proposal for a national programme on patient safety improvement for Switzerland, available at http://www.swiss-q.org/apr-2001/docs/Final_ReportE.pdf, accessed January 2003

Burns F. (1998), Information for health: information strategy for the modern NHS 1998-2005, NHS Executive available at http://www.doh.gov.uk/ipu/strategy/summary/execsum.pdf

Carnall D., (1998), NHS information strategy launched, British Medical Journal, vol: 317, pp 901

Carter M (1998), Should patients have access to their medical records? The Medical Journal of Australia, vol: 169, pp 596-597

Carter M (2000) Integrated electronic health records and patient privacy: possible benefits but real dangers, The Medical Journal of Australia, vol. 172, pp 28-30

Chassin M. R., Becher E.C. (2002), The Wrong Patient, Annals of Internal Medicine, June, vol 136, is. 11, pp. 826-833

Clayton P. D. (2001), The state of clinical information systems after four decades of effort, Yearbook of Medical Informatics, pp 333- 337

Cohen A. (2003), Smart cards, smarter health care, PC Magazine, October, available at http://www.pcmag.com/ article2/0,4149,1265720,00.asp

Coiera E. (2000),When conversation is better than communication, Journal American Medical Informatics Association, vol. 7, is. 3, pp. 277-286

Coiera E., Clarke R. (2003), “e-Consent”: the design and implementation of consumer consent mechanisms in an electronic environment, Journal of American Medical Informatics Association, PrePrint published December 7, 2003; doi:10.1197/jamia.M1480

Commonwealth of Australia (2003), HealthConnect Interim research report, available at http://www.health.gov.au/healthconnect/researchrep/irr.html accessed January 2004

Confidentiality of Medical Records (1998): A situation analysis and AHIMA's position,American Health Information Management Association, www.ahima.org/infocenter/current/white.paper.html accessed February 2001

Connolly C. (2005), Cedars- Sinai Doctors Cling to Pen and Paper, Washington Post, 21 March 2005, p. A01

Cornwall A. (2000), NSW electronic health records get serious, Privacy law and policy reporter, available at http://www.austlii.edu.au/au/journals.OLD/PLPR/2000/42.html

Cotter J. (2003), Alberta health providers to share medical records via computer, Canadian Press, October 25, 2003

Cox S., and Cox T. (1996), Hazard, harm and risk: the basic equation, in: *Safety Systems and People*, Reed Educational and Professional Publishing Ltd.

Cox P (2001), Using patient identifiable data without consent, The British Medical Journal, vol. 322, pp 858

Creswell J. W. (1994), Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research, Prentice Hall, p. 94

Creswell J. W. (2003), Research Design: Qualitative, Quantitative and Mixed Methods Approaches, second edition, Thousand Oaks, California, Sage publication

Cushman R. (1997), Serious Technology Assessment for Health Care Information Technology, Journal of the American Medical Informatics Association, vol. 4, is. 4, pp 259-265

Dalla-Vorgia P., Lascaratos J., Skiadas P., and Garanis-Papadatos (2001), Is consent in medicine a concept only of modern times?, Journal of medical ethics, vol. 27, pp. 59-61

Dash J. (2001), VA hospitals test smart cards for patient information, Computerworld, available at http://www.computerworld.com/securitytopics/security/ privacy/story/0,10801,60471,00.html accessed January 2004

Data Protection Act 1998, http://www.hmso.gov.uk/acts/acts1998/19980029.htm accessed 23 May 2001

Davis P., Lay-Yee R., Briant R., Schug S., Scott A.,Johnson S., Bingley W. (2001), Adverse events in New Zealand Public hospitals: Principal findings from a National Survey, occasional paper, December 2001, the Ministry of Health, Wellington, New Zealand

Dearne K(2001), Prescribing a privacy cure, Australian IT, May 1, pp 44

Department of Health Expert Group (2000), An Organisation with a memory, Report of an expert group on learning from adverse events in the NHS chaired by the Chief Medical Officer, Crown Copyright, UK., available at http://www.doh.gov.uk/cmo/orgmem.pdf, accessed January 2003

Dick R, Steen E. (1991), The computer based patient record: an essential technology for healthcare. US National Academy of Sciences, Institute of Medicine.

Dini E. F., Linkins R. W., Sigafoos J. (2001), The impact of computer generated messages on childhood immunization coverage, Year book of medical informatics, pp. 210-217

Draft health privacy guidelines (2001), The consultation document issued by the office of the federal privacy commissioner, Sydney, NSW
http://www.privacy.gov.au/rfc/index.html accessed 21 May 2001

Dudeck J. (2001), Informed consent for cancer registration, Lancet Oncology, vol.2, pp 8-9.

EHR Working Group (2001), A NSW Health Strategy for the Electronic Health Record, A working group of the Information Management Implementation Co-

ordination Group, available at
http://www.ciap.health.nsw.gov.au/documents/NSW_EHR_Strategy.pdf
accessed March 2003

E1714-00, Standard Guide for a properties of a Universal Healthcare Identifier, The American Society for Testing and Materials

Evans B, Ramay C. N. (2001), Integrity of communicable disease surveillance is important patient care, the British Medical Journal, vol. 322, pp 858

Eysenbach G, (2000) Consumer health informatics: recent advances, British Medical Journal, 320,pp 1713-1716

Falla M. (1995), *Managing Collaborative R& D Projects*, Engineering Management Journal, vol. 5, is. 6, pp267-272.

Fine L.G., Keogh B. E., Cretin S., Orlando M., Gould M. M. (2003), How to evaluate and improve the quality and credibility of an outcomes database: validation and feedback study on the UK Cardiac Surgery Experience, The British Medical Journal, vol 326, pp25-28

Finkelstein A. (1993), Report of the inquiry into the London Ambulance Service, International Workshop on Software Specification and Design Case Study, available at

http://www.cs.ucl.ac.uk/staff/a.finkelstein/las/lascase0.9.pdf accessed February 2002

Finkelstein A., Dowell J. (1996), A Comedy of Errors: the London Ambulance Service case study, Proceedings of the 8th International Workshop on Software Specification and Design (IWSSD'96), Germany, available at www.cs.ucl.ac.uk/staff/A.Finkelstein/las.html

Friedman C.P., Wyatt J.C. (1997), Evaluation as a field, In: Evaluation methods in medical informatics, Springer-Verlag New York, pp.17-63

Gaithersburg I.V. (2000), Electronic Medical Records and Patient Privacy, The Health Care Manager, March pp 63-69

Garfinkel S (2000), Computerized patient records: the threat: In: Database Nation, The death of privacy in the 21st century, pp 149-151

Gerber P(1999), Medicine and the law: Confidentiality and the courts, The Medical Journal of Australia, vol. 170 pp 222-224

Gosbee J. (2002), Human factors engineering and patient safety, Quality and safety in healthcare, vol.11, pp.352-354

Gostin L.O., Turek-Brezina J., Powers M., Kozloff R., Faden R., Steinauer D.D. (1993), Privacy and Security of Personal Information in a New Health Care

System, Journal of American Medical Association, vol. 270, no. 20, pp 2487-2493

Grant J.B., Hayes R. P., Pates R. D., Elward K. S., Ballard D.J. (1996), HCFA's Health care quality improvement program: The medical informatics challenge, Journal of the American Medical Informatics Association, vol.3, no.1, pp 15-26

Greenes R. A. and Shortliffe E. H. (1990), Medical informatics: An emerging academic discipline and institutional priority, Journal of American Medical Association, vol. 263, is. 8., pp 1114-20

Guidelines under section 95 of Privacy Act 1988 (March 2000), Common wealth of Australia, http://www.health.gov.au/nhmrc/publicat/pdf/e26.pdf accessed April 2001

Halbach J.L., Sullivan L (2002), Medical errors and Patient Safety: A curriculum guide for teaching medical students and family practice residents, New York Medical College: Department of Family Medicine

Halldorsson M, Cavelaars A E, Khnst AE, Mackenbach JP, Socioeconomic differences in health and well-being of Children and adolescents in Iceland, Scand J Public Health, vol 27 (1999) 43-47

HB-228-2001, Standards Australia (2001), Guidelines for managing risk in healthcare, Australian/New Zealand Handbook, Standards Australia, ISBN 0 7337 34197, www.standards.com.au accessed 13 May 2002

HealthConnect Program Office (2002), Health Connect Project Overview, available at http://www.health.gov.au/healthconnect/pdf_docs/projovw.pdf accessed December 2003

Health Information Management Association of Australia Limited (HIMAA), (2001), Annual Report 2000-2001, ABN 54 008 451 910 http://www.himaa.org.au

Herald Sun news (2003), Health smart cards within five years, Herald Sun, 14 November 2003, available at http://heraldsun.news.com.au/common/story_page/0,5478,7865295%5E1702,00.html, accessed January 2004

Hier D. B., Rothschild A., LeMaistre A., Keeler J. (2005), Differing faculty and housestaff acceptance of an electronic health record, International Journal of Medical Informatics Association, doi:10.1016/j.ijmedinf.2005.03.006

Hippisley-Cox J., Pringle M., Cater R., Wynn A., Hammersley V., Coupland C., Hapgood R., Horsfield P., Teasdale S., Johnson C. (2003), vol. 326, pp. 1439-1443

Holtzman N. A. (2004), Computerized Order Entry Leads to Unwanted Testing, Current Cases and Commentaries : Clinical Ethics, available at http://webmm.ahrq.go/ accessed December 2004

Hornby A. S. and Wehmeier S. (1989), Oxford Advanced Learner's Dictionary, Oxford University Press

Hornsey J., Friend C. (2003), Community Health Electronic Medical Record and Telehealth: A Future Convergence, Proceedings of 8th NSW Telehealth Initiative Symposium 2003, Sydney, September 4, 2003

House E.R. (1980), Evaluating with validity, Beverley Hills: Sage.

House of Representatives Standing Committee on Legal and Constitutional Affairs (2000), Patient access to medical records, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000, The Parliament of the Commonwealth of Australia, June pp 75-85

Hudson P. (2003), Applying the lessons of high risk industries to health care, Quality and safety in healthcare, vol.12, pp 7i-12

Huff S.M. (1998), Clinical Data Exchange Standards and Vocabularies for Messages. *Journal of American Medical Informatics Association*, AMIA Annual Fall Symposium Supplement, pp. 62-67

Humpherys B.L. (2000), Electronic health record meets digital library: A new environment for achieving an old goal, JAMIA, vol. 7, no. 5, Sept, Oct

IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, http://www.iec.ch/61508/ accessed December 2000

Institute of Medicine (1997), The Computer Based Patient Record: An essential Technology for healthcare. Eds. Dick R.S., Steen E.B., Detmer D.E., National Academy Press

Institute of Medicine (2000), Doing what counts for patient safety: Federal Actions to reduce medical error and their impact, Report of Quality Interagency Coordination Task Force to the President,
http://www.quic.gov/report/mederr2.htm

Institute of Medicine (2001), Crossing the quality chasm: A New Health System for the 21st Century, Committee on Quality of Health Care in America, National Academy Press, Washington, D.C.

Institute of Medicine (2003), Committee on Data Standards for Patient Safety: Board on health care services (2003), Key capabilities of an Electronic health record system: letter report, The National Academy of Sciences, available at http://www.nap.edu/openbook/N1000427/html/R1.html accessed 8 August 2003

International Associations of Classification Societies (1999), Formal safety assessment, available at http://www.iacs.org.uk/fsa/wp5/fsaglossary.htm

International Commission on Large Dams (ICOLD) 2002., Risk assessment in Dam Safety Management: A Reconnaissance of Benefits, Methods and Current Applications. ICOLD Bulletin Draft, December

Iiripcsak G., Wilcox A. (2002), Reference standards, judges, and comparison subjects: roles for evaluating experts in evaluating system performance, Journal of American Medical Informatics Association, vol. 9, is.1, pp 1-15

Ingelfinger J.R., Drazen J.M. (2004), Registry Research and Medical Privacy, The New England Journal of Medicine, Apr 1, vol. 350, iss 14, pp 1452

Institute for Safe Medication Practices (2003), ISMP list of error-prone abbreviations, symbols, and dose designations, Medication Safety Alert, vol 8, is 24, available at http://www.ismp.org/PDF/ISMPAbbreviations.pdf?itemID=21576

ISMP (2003), Double checks for endogenous and exogenous errors, Medication Safety Alert October 30, 2003, available at http://www.ismp.org/MSAarticles/double.htm accessed November 2003

ISMP (2003), Intrathecal injection of ionic contrast media may be fatal, Medication Safety Alert November, available at

http://www.ismp.org/MSArticles/fatal.htm accessed January 2004

ISMP (2003), Looks like a problem: ephedrine – epinephrine, Medication Safety Alert April 17, 2003, available at http://www.ismp.org/MSAarticles/looks.htm accessed August 2003

Jerant A.F., Hill D.B., (2000), Does the use of electronic medical records improve surrogate patient outcomes in outpatient settings? Journal of Family Practice, April 2000, vol. 49, is. 4, pp 349

Jurgens R. (2001), HIV testing and confidentiality: final report, Canadian HIV/AIDS Legal Network & Canadian AIDS Society, available at http://www.aids-hepatitisc.org/stigma/Hepatitis/HIV-testing-and-confidentiality.htm

Kaplan B., Brennan P.F. (2001), Consumer Informatics supporting patients as co-producers of quality, Journal of American Medical Informatics Association, Vol 8, no.4, pp 309-316

Kashual R. and Bates D. W. (2002), Information technology and medication safety: what is the benefit?, Quality and safety in healthcare, vol:11, pp 261-265

Kaushal R. (2003), Child Receives Overdose of Phenytoin Due to Ambiguous Use of Abbreviations, Agency for healthcare research and quality, April 2003,

available at http://www.webmm.ahrq.gov/cases.aspx?ic=9, accessed October 2003

Kim M.I., Johnson K.B. (2002), Personal health records: evaluation of functionality and utility, Journal of American Medical Informatics Association, vol:9. is. 2, pp 171-180

Knoppers BM (2000), Confidentiality of Health Information: International Comparative Approaches, A Health Information Network for Australia, Report to Health Ministers by the National Electronic Health Records Taskforce, Commonwealth of Australia

Kohn L. T., Corrigan J. M., Donaldson M. S. (2000), To Err is Human: Building a Safer Health System, National Academy Press, Washington D.C.

Kuhn K.A., Giuse D. A. (2001), From Hospital Information Systems to Health Information Systems- Problems, Challenges, Perspectives, Year Book of Medical Informatics, pp 63-76

Langberg M. L. (2003), Challenges to implementing CPOE: A case study of a work in progress at Cedars-Sinai, Modern Physician, February 2003, pp21-22 available at http://www.modernphysician.com/page.cm?pageId=216 accessed December 2003

Laprie J.C., (1995), Dependable computing: concepts, limits, challenges, 25th IEEE International Symposium on Fault tolerant computing- special issue, pp. 42-54, Pasadena, California, USA, IEEE

Lesar T.S., Briceland, L.L., Delcoure K., Parmalee J.C., Masta-Gornic V and Pohl H. (1990), Medication prescribing errors in a teaching hospital. Journal of American Medical Association, vol. 263: pp 17.

Leveson N. G. (2003), White paper on approaches to safety engineering, available at http://sunnyday.mit.edu/caib/concepts.pdf accessed May 2004.

Leveson N. G. (1995), Safeware: System Safety and Computers, Addison-Wesley publishing company, Reading, MA.

Lippeveld T., Sauerborn R., (2000), A framework for designing health information systems, In: Design and Implementation of health information systems, ed. Lippeveld T., Sauerborn R, Bodart C., World Health Organisation, Geneva, pp. 15-32

Livingston A.D., Jackson G., Priestley (2001), Root cause analysis: literature review, WS Atkins Consultants Ltd, ISBN 0717619664, http://www.hse.gov.uk/research/crr-pdf/2001/crr01325.pdf

Marx D. A. and Slonim A. D. (2003), Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modeling in health care, Quality and safety in health care, vol.12 (suppl II),pp ii33 –ii38

Mandl KD, Szolovits P, Kohane IS (2000), Public standards and patients' control: how to keep electronic medical records accessible but private, vol. 322, pp 283-287

Mandl K.D., Lee T.H. (2002), Integrating medical informatics and health services research: the need for dual training at the clinical health systems and policy levels, Journal of American Medical Informatics Association, vol.9, no.2, pp 127-132

McDonald C., (2002), IOM Patient Safety Standards Workshop, September 23, 2002, Committee on Patient Safety Data Standards, Second Meeting and Workshop, Washington, D. C. available at http://www.iom.edu/IOM/IOMHome.nsf/Pages/PSDS+Meeting+two+and+Workshop

Medical Record Privacy (1999), Electronic Privacy Information Center, http://www.epic.org/privacy/medical accessed 17 May 2001

Miller P.L., Frawley S. J., Sayward F.G. (2001), Exploring the utility of demographic data and vaccination history data in the deduplication of

immunization registry Patient Records, Journal of Biomedical Informatics, vol. 34, pp 37-50

Moczygemba J., Hewitt B. (2001), Managing clinical data in an electronic environment, Health Care Manager, vol.19, is. 4, pp 33-38

Murff H. J.and Kannry J. (2001), Physician Satisfaction with Two Order Entry Systems**,** Journal of American Medical Informatics Association**,** vol.8, is.5, pp. 499-511

Murphy G. and Brandt M. (2000), Health Informatics Standards and Information Transfer: Exploring the HIM Role, Journal of AHIMA, American Health informatics Management Association, http://www.ahima.org/journal/pb/01.01.html

Murray D (2001), Health privacy botched, information week, April, pp14-18

Myers M.D. (1997), Qualitative research in information system, MISQ Discovery, June, available at http://www.qual.auckland.ac.nz accessed April 2005

National Committee on Vital and Health Statistics (2000), Report to the Secretary of Department of Health and Human Services on Uniform Data

Standards for Patient Medical Record Information, July, Available at http://ncvhs.hhs.gov/hipaa000706.pdf accessed March 2001

National Electronic Health Record Taskforce (2000), A Health Information Network for Australia, Commonwealth of Australia, http://www.health.gov.au/healthonline/ehr_rep.pdf accessed October 2000

National Health Service Executive (NHS 1998), Information for Health: An Information Strategy for the Modern NHS 1998-2005, HMSO, London.

Neumann P.G. (1989), The computer-related risk of the year: misplaced trust in computer system, IEEE Computer Assurance1989 (COMPASS '89), Proceedings of the Fourth Annual Conference on 'Systems Integrity, Software Safety and Process Security', 19-23 June 1989, pp:9 – 13

Neumann P.G. (1995), Computer Related Risks, Addison Wesley Publishing company, ACM Press, Reading Massachusetts

NSW Minister Advisory Committee on Privacy and Health Information (2000), Panacea or Placebo? Linked Electronic Health Records and Improvement in Health Outcomes, December

Nosworthy J. D. (2000), A practical risk analysis approach: Managing BCM Risk, Computer and Security, vol:19, is. 17, pp 596-614

Nieva V.F. and Sorra J. (2003), Safety culture assessment: a tool for improving patient safety in healthcare organizations, Quality and Safety in health care, vol. 12, pp.17ii-23

O'Brien M.C. and Yearwood J.L. (2003), Insights into consumer decisions surrounding adverse drug reactions: Some preliminary results, Eleventh National Health Informatics Conference HIC2003, Sydney, Australia

Ornstein C. (2003), California; Hospital Heeds Doctors, Suspends Use of Software; Los Angeles Times, January 22, 2003, pp 2, available at http://www.latimes.com/news/printedition/california/la-me-cedars22jan22,0,1528318.story?coll=la-headlines-pe-california/ accessed January 2003

Payne T. H., Hoey P. J., Nichol P., and Lovis C., Preparation and use of preconstructed orders, order sets, and order menus in a computerized provider order entry system, Journal of American Medical Informatics association, vol.10, is.4, pp 322- 329

Perreault LE and Wiederhold G (1990), System Design and Evaluation, in: Medical Informatics: Computer applications in health care, Shortliffe EH, Perreault LE (eds) Addison Wesley Publishing, Reading , MA. pp. 154

Phung H, Young L, Tran M, Win K.T. Alcock C, Hillman K. (2004), Health informatics and health information management in maternal and child health services, Health Information Management Journal, vol. 33, is. 2, pp. 36-42

Pressman R. S.(2000), Software Engineering: A Practitioner's Approach, Fifth Edition, McGraw Hill, New York

Pronovost P. J., Weast B., Holzmueller C. G., Rosenstein B. J., Kidwell R. P., Haller K. B., Feroli E. R, Sexton J. B., Rubin H. R. (2003), Evaluation of the culture of safety: survey of clinicians and managers in an academic medical center, Quality and Safety in Health Care, vol.12, pp 405-410

Purdy, B.D. (2000). Medication errors in the HIV-infected population, Medscape Pharmacists, available at http://primary.medscape.com/med…n06/mph7403.purd/mph7403.purd.html accessed October 2003

Puplick C. (2003), The privacy implications of the revolution in health technologies, Australian Financial Review 5th Annual Congress

Reason J (1990). Human error, New York: Cambridge University Press,

Reason J., (2000), Human errors: model and management, British Medical Journal, vol. 320, pp 768-770

Rector A. L., Nolan W. A., Kay S. (1991), Foundations for an Electronic Medical Record, Methods of Information in Medicine, vol. 30: pp. 179-86.

Redmill F. (1993), Software in safety-critical applications- a review of current issues, ed.Redmill F. and Anderson T., Safety-critical Systems: current issues, techniques and standards, Chapman & Hall,London, pp 3-15

Relex Software Corporation (2001), Visual Reliability Software, available at www.fault-tree.com accessed November 2001

Reykjavik (2000), Iceland sells its medical records, pitting privacy against greater good, CNN news, http://www.cnn.com/2000/WORLD/europe/03/03/iceland.genes, accessed 17 May 2001

Rigby M., Roberts R., Williams J., Clark J., Savill A., Lervy B., Mooney G. (1998), Integrated record keeping as an essential aspect of a primary care led health services, British Medical Journal, vol. 317, pp 579-582

Rind DM, Kohane IS, Szolovits P, Safran C, Chueh H, Barnett O (1997), Maintaining the confidentiality of medical records shared over the internet and the world wide web, Annals of Internal Medicine, vol. 127, pp 138-141

Robert E. Nolan company (2003), Replacing ICD-9-CM with ICD-10-CM and ICD-10-PCS Challenges, Estimated Costs and Potential Benefits, October available at http://vocuspr.vocus.com/VocusPR30/Temp/{cd11d011-fb5c-42f8-a9d7-9f3160d5af31}/031030_BCBSA_Nolan_ICD-10_Study.pdf

Roberts L. and Wilson S. (2001), Argument for consent may invalidate research and stigmatize some patients, The British Medical Journal, vol. 322, p 858 (1 page)

Rothschild J. (2001), EMR's making noise thanks to voice recognition programs, Dermatology Times, vol: 22, is. 2, p 14 (1 page)

Runciman W. B. (2002), Lessons from the Australian Patient Safety Foundation: setting up a national patient safety surveillance system-is this the right model?, Quality and safety in health care, vol.11, pp 246-251

Safety and Quality Council (2003), Patient Safety: Towards sustainable improvement: Fourth Report to the Australian Minister's Conference, July 31, available at http://www.safetyandquality.org/articles/Publications/patientsafejul03.pdf accessed December 2003

Sauerborn R. (2000), Using Information to make decisions, In: Design and Implementation of health information systems, ed. Lippeveld T., Sauerborn R, Bodart C., World Health Organisation, Geneva, pp 33-48

Schiffman R. N., Brandt C. A., Liaw Y., Corb G. J. (1999), A design model for computer based guideline implementation based on information management services, Journal of the American Medical Informatics Association, vol. 6, no.2, pp. 99-103.

Schloeffel P. and Jeselon P. (2002), ISO/TC 215 Ad Hoc Group Report, Standards Requirements for the Electronic Health Record and Discharge/ Referral Plans: Final Report, available at http://www.gpcg.org/publications/docs/IS0_EHR_FinalReport.pdf, accessed 22nd April 2003

Schoenberg R, Safran C (2000), Internet based repository of medical records that retains patient confidentiality, British Medical Journal, vol. 321, pp 1199-1203

Sharbo A. (2004), Structuring the Medical Narrative in Patient Records- A further Step Towards a Multiaccessible EHR, Yearbook of Medical Informatics 2004, pp. 317-320

Shojania K. G. (2003), Mr Smith" Mix-up: Patient Almost Receives Haloperidol Ordered for Roommate With Same Last Name, Agency for healthcare research

and Quality, February 2003, available at

http://www.webmm.ahrq.gov/cases.aspx?ic=1#Table accessed October 2003

Shortliffe E.H., Barnett G.O. (2001), Medical data: their acquisition, storage, and use, In: Medical Informatics:Computer Applications in health care and biomedicine, ed. Shortliffe E.H., Perreault L.E., second edition, Springer, New York

Shortliffe E. H., Perreault L.E. (1990), Medical Informatics: Computer Application in healthcare, Addison-Wesley Publishing Company, Reading Massechusset

Shortliffe E.H., Blois M.S (2001). The Computer Meets Medicine and Biology: Emergence of a Discipline. Chapter 1. In: Shortliffe E.H. , Perreault L.E. (eds) Medical Informatics: Computer Applications in Health Care and Biomedicine. New York: Springer-Verlag, 2001.

Singer S. J., Gaba D. M., Geppert J.J., Sinaiko A.D., Howard S.K., Park K.C. (2003), The culture of safety: results of an organization-wide survey in 15 California hospitals, Quality and safety in health care, vol.12, pp. 112-118

Sommerville I (2001), Software Engineering, sixth edition, Addison Wesley, Reading, Mass.

Spann S. J. (1990), Should the complete medical record be computerized in family practice? An affirmative view - Controversies in Family Practice, Journal of Family Practice, April

Stake R. E. (1995), The Art of Case Study Research, Sage Publications, Thousand Oaks, California.

Stein L. (1997), The electronic medical record: promises and threats, web security: A matter of trust, web journal, o'Reilly & Associates, vol.2, is. 3, available at http://www.oreilly.com/catalog/wjsum97/excerpt/

Sullivan F., Mitchell E. (1995), Has general practice computing made a difference to patient care? A systematic review of published reports, British Medical Journal, vol:311, pp 848-852

Swiss Federal Institute of Technology (2003), risk definitions, available at http://www.isn.ethz.ch/crn/risk_issues/documents/risk-definitions.pdf

Szolovits P. (1995), A revolution in electronic medical record systems via the world wide web, In Proceedings of the International Association for the advancement of health information technology, Geneva, Switzerland, September 6-8

Tang P. C., LaRosa M. P., Gordon S. M. (2001), Use of computer-based records, completeness of documentation, and appropriateness of documented clinical decisions, Year book of medical informatics, pp. 300-306

Tange H. J., Hasman A., Robbe P. Fd V., Schouten H. C. (1998), Medical narratives in electronic medical records, Yearbook of Medical Informatics, pp 230-251

Tellis W. (1997), Application of a case study methodology, The Qualitative Report, vol. 3, no.3 available at http://www.nova.edu/ssss/QR/QR3-3/tellis2.html accessed April 2005

Thane H. (1997), Safe and reliable computer control systems on overview, In: Safe Comp97: Proceedings of the 16th International conference on Computer Safety, Reliability and Security, York, 7-10 September 1997, ed. Daniel P., Springer

The Oath By Hippocrates, 4th Century B.CE available at http://classics.mit.edu/Hippocrates/hippooath.html accessed November 2003

U.S. National Archives and Record Administration (2000), The Soundex indexing system, available at www.archives.gov/research_room/ genealogy/census/soundex.html

Van-Bemmel J.H. and Musen M.A. (1997), Handbook of Medical Informatics, AW Houten, Netherlands : Bohn Stafleu Van Loghum ; Heidelberg, Germany : Springer Verlag

VA National Centre for Patient Safety (2003), Healthcare failure Mode and Effect Analysis Course Material, available at http://www.patientsafety.gov

Velde R. Vd (2000), Framework for a clinical information system, International Journal of Medical Informatics, vol: 57, pp 57-72

Vindal Y. (2003), Report of a 27-Year Observational Study on Medical Errors and Systemic Failures Within the Health-care System, available at http://www.101waystopreventerrors.com/report1a.htm accessed January 2004

Waegemann CP (2000), A Matter of Privacy for ehealth: Security Policies - International Privacy - Internet Security
http://www.medrecinst.com/conferences/asia/proceedings/10-00/privacy.pdf
accessed May 2001

Waegemann C. P. (2002), Status report 2002: Electronic Health Records, available at http://www.medrecinst.com/resources/ehr2002/StatusReport.pdf, accessed September 2003

Wainwright D and Warning T (2000), The information Management and Technology Strategy of UK National Health Services: Determining Progress in

the NHS acute hospital sector, The International Journal of Public Sector Management, vol. 13, no:3, pp 241-259

Wainwright M. (2001), NHS faces huge damages bill after millennium bug error, Guardian, available at http://www.guardian.co.uk/Archive/Article/0,4273,4257065,00.html accessed 17 September 2001

Wang R.Y., Strong D.M. (1996), Beyond accuracy: What data quality means to data consumers, Journal of Management Information Systems, vol. 12, is. 4, pp 5

Warren J., Stanek J., Gadzhanova S., Misan G. (2003), General Practice Data Mining- Making the best of practical and fundamental limitations, Proceedings of HIC 2003 RACGP 12CC Combined Conferences, Sydney, Australia

Weingart S. N., Wilson R. M., Gibberd R. W., Harrison B. (2000), Epidemiology of medical error, British Medical Journal, vol. 320, pp 774-777

Weinger B. M. and Slagle J. (2002), Human Factors Research in Anesthesia Patient Safety: Techniques to Elucidate Factors Affecting Clinical Task Performance and Decision Making, Journal of American Medical Informatics Association, vol. 9 (90061):S58-S63; doi:10.1197/jamia.M1229

Weir C. R., Hurdle J. F., Felgar M. A., Hoffman J. M., Roth B., Nebeker J. R. (2003), Diret Text Entry in electronic Progress Notes: An evaluation of Input Errors, Methods of Information in Medicine, vol. 42, is. 1, pp. 61-67

Wigertz O.B. (2001), Synopsis: Computer-based patient records, Year book of medical informatics, pp. 259-262.

Win K.T., (2004), Identifying the Risk assessment method applicable to the electronic health record systems, Proceedings of HIC2004,Brisbane, July 2004

Win K.T., Croll P., Cooper J., Alcock C. (2002), Issues of Privacy, Confidentiality and Access in Electronic Health Record, Journal of Law and Information Science, vol. 12, is. 1, pp24-45

Win K.T., Croll P., Cooper J. (2002), Setting a safety standards for electronic medical records, Proceedings of HIC2002, The Tenth Annual Health Informatics Conference, Melbourne, Australia, August 4- 6.

Win K.T., Song H., Croll P., Cooper J. (2002), Implementing patient's consent in electronic health record systems, Proceedings of CollECTeR 2002, Melbourne, Australia., December 1, 2,2002

Win K.T., Croll P., Cooper J., (2003), Dependability: Important factor for the success of electronic health record systems, Proceedings of The eleventh Annual

Health Informatics Conference, Darling Harbour, Sydney, Australia, 10 –12 August

Win K.T., Croll P., Cooper J., (2003), Privacy, confidentiality and consent of electronic health record systems, Proceedings of The eleventh Annual Health Informatics Conference, Darling Harbour, Sydney, Australia, 10 –12 August

Win K.T., Croll P.(2005), Engineering Dependable Health Information Systems, In: Creating knowledge based healthcare organization, editors: Wickramsinghe N., Gupta J.N.D., Sharma S. K., IDEA Group Inc., Hershey, PA. ,pp 91- 109

Win K.T., Selakovic G. (2004), Evaluative study of Web Based Personal Health Record Systems, Proceedings of CollECTeR2004 Workshop, Adelaide, May 7-8

Wong D. A. (2002), It's more than human error- A system approach to patient safety, Spineline, vol 3. is. 3, pp 20-21, available at http://www.spine.org/Forms/Patient_Safety_Systems_Approach.pdf accessed January 2004

Yin R. K.. (1994), Case Study Research: Design and Methods,second edition., Applied Social Research Methods Series, vol.5, SAGE publications, Thousand Oaks, California

Zalud B. (2003), Smart card breakthrough?, Security, available at http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,112205,00.html

Zviran M., Ahituv N. and Glezer C. (2003), A Conceptual Model for Increasing Utilization of Dependable Computer Networks, Data and Knowledge Engineering, Vol. 46, No. 3, September, pp. 247-269

Appendix

Please see print copy for Appendices