RISK ASSESSMENT OF ELECTRONIC HEALTH RECORD SYSTEM

Khin Than Win and Carole Alcock
School of IT and Computer Science
University of Wollongong
win@uow.edu.au

Joan Cooper
Flinders University
Joan.cooper@flinders.edu.au

ABSTRACT

This research aims to develop a framework for safety and dependability of the electronic health record systems (EHRs) in order to analyse the risks associated with EHRs. The research identifies the safety attributes of EHRs by identifying the framework of dependability and data quality of EHRs. The research explores risk assessment methods and identifies the risk assessment method for the EHRs

INTRODUCTION

Medical errors are of growing concern in the health care industry. As electronic health records are now part of the healthcare system, a necessary requirement is that electronic health records (EHRs) are safe and dependable. Therefore this research aims to develop a framework for safety and dependability of EHRs in order to analyse the risks associated with electronic health record systems. There is no risk assessment of electronic health record system conducted previously in healthcare and the study risk assessment of EHRs would be a significant contribution to the health care industry.

The research will identify a relationship framework for dependability, data quality and attributes for safety assessment of EHRs. The research involves (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 the EHRs and (iv) drawing conclusions based on the above findings.

DEVELOPING A THEORETICAL BASIS OF SAFETY

The release of the report “To Err is Human: Building a Safer Health System” (Kohn et al. 2000), emphasised the importance of safety in heath care.. There have been many reports of medical misadventure, for example 98,000 Americans die each year as a result of preventable medical errors (Kohn et. al. 2000). The 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 work place (IOM 2000). The National Survey of New Zealand (1998) has documented the 4.5% of all admissions were associated with highly preventable adverse events (Davis et. al 2001). In Australia, 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). The following list comprises the system attributes and functionality required to ensure confidence in the safety of the system:

Data Attributes

- Dependability

  Attributes of dependability include: availability, reliability, security and safety (Sommerville 2001).
- Quality

  Data quality is important because having appropriate information will assist in the decision making process.
- Data Quality and dependability

  Table 1 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.

Appropriate	Inappropriate	Dependability	Measures
Data accuracy	Inaccurate information by mistake	Reliability	Validation check
	Inaccurate information by software	Security, Reliability	Quality control
	Inaccurate information by intention	Security	Proper security measures
Data accessibility	Data not accessible due to destruction of data	Availability, Security, Safety	Security measures
	Data not accessible due to accidental destruction	Reliability	Authentication check, safety procedures
	Data not accessible due to intentional manipulation	Security, Reliability	
	Data inaccessible due to malfunction in hardware or software	Availability, reliability	
	Data inaccessible due to location of information unknown	Availability	
Data consistency	Different value to same logical data Different units Inconsistent semantics	Reliability	Implementing data standards Interoperability checks
Data comprehensiveness	Missing data	Availability, reliability	Ensure data integrity
	Incomplete data due to incomplete transfer	Reliability	
	System not functioning properly	Availability, reliability, safety	
Data currency	Inaccurate data value	Reliability	Appropriate data field

Table 1: Relationship of Data quality and dependability (Win et. al 2002)

- Accuracy (generated by software)

  In the United Kingdom, because of the millennium bug error, incorrect Down syndrome test results were sent to 154 pregnant women. As a result four Down syndrome babies were born to mothers the tests of whom put them in the low risk group. Two terminations were carried out as a result of this mistaken test report (Wainwright 2001).
- Accuracy (information in error)

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

  In one incident, a lack of data comparability standards resulted in a patient having a severe reaction to 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).
- Data granularity

There can be a significant difference if the data value is not entered or displayed fully. 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.

- Unique Patient Identification

  Unique identification would allow for the rapid and accurate identification of patient. It will prevent duplication of records and enhance efficient patient care. Health care procedures such as invasive testing, blood transfusions and surgical procedures require accurate identification of the patient and wrong identification could lead to disastrous outcomes.

Data Entry.

Clearly an important consideration in ensuring the quality of data is the method of entry. There are a plethora of methods by which this may occur. Data may be handwritten into the medical chart and scanned later. Equally data may be entered through voice recognition software, pen pad, mouse or touch screen. Possible errors during data entry include the following. If the data is transcribed or scanned from the handwritten document and if the handwriting is illegible, the data entered may be incorrect. . If the data is transcribed or scanned after the patient is discharged from the hospital or after the treatment has been given, the erroneous data would have impact for the future research or future treatment or public health purposes. But if it is before the treatment there may be immediate repercussions to the health of the patient. For example, suppose the handwriting was wrongly interpreted for 'i.v' to 'i.t'. There is a great difference in giving the dose intravenously as distinct from intrathecally. In an incident in Denver, for example,, an infant death occurred because benzathine penicillin for 'i.m.' (intramuscular) injection was ordered incorrectly as 'i.v.' (intravascular) (Kaushal and Bates 2002).

Abbreviations should be used cautiously as there can be errors of misinterpretation. The following list is the some examples of error-prone abbreviations, symbols and dose designations provided by the Institute for Safety Medication Practices (ISMP) (ISMP 2003).

Abbreviations	Intended Meaning	Misinterpretation	Correction
µg	Microgram	Mistaken as mg	Use "mcg"
AD, AS, AU	Right ear, left ear, each ear	Mistaken as OD, OS, OU (right eye, left eye, each eye)	Use "right ear", "left ear", or "each ear"
BT	bedtime	Mistaken as "BID" (twice daily)	Use "Bedtime"
ij	injection	Mistaken as "IV" or "intrajugular"	Use "injection"
HS hs	Half-strength At bed time, hours of sleep	Mistaken as "bedtime" Mistaken as half-strength	Use "half-strength" or "bed time"
q.o.d	Every other day	Mistaken as "q.d."(daily) or "q.i.d" (four times daily)	Use every other day
AZT	Zidovudine (Retrovir)	Mistaken as Azathioprine	Use complete drug name
HCT	Hydrocortisone	Mistaken as hydrochlorothiazide	Use complete drug name

Table 2: 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 may have a serious impact on the patient if the wrong medication is administered mistakenly. For example, , a 31-year-old man died as a result of wrong injection of contrast-media intrathecally for the 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 causing muscle spasms, convulsions and death (ISMP 2003).

Erroneous interpretation of medication dose could also have serious health consequences. . In some electronic health record systems, clinical notes are still entered in plain text format and systems are not integrated with 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 written as ‘mg/kg/d’ without specification that ‘d’ meant ‘day’ vs. ‘dose’ (Kaushal 2003). Therefore, checks need to be built into the software as a safeguard against the possible combined effects of the medication, suggested routes of administration for each drug, and drug potentiation effects.

Data can be keyed into wrong patient records and there could be a possibility of wrong treatment, wrong discharge, wrong operation, missed monitoring depending on the condition and nature of mixed cases. Therefore, in electronic health record systems, patients’ names and identifications should be displayed on all screens to minimise incorrect data entry. If the data is entered wrongly for male and female, for example, there can be consequences in reminders for such events as mammography, pap smears, prostate screening based on the gender of the patient. Data verification and validation checks during the data entry will improve the reliability of the data. For example, adding algorithms that check against the patient’s age and weight can prevent erroneous entry of patients’ data. If the person’s age and weight entered is in unacceptable range, the system will prompt the alert message so that the care provider will know and decide immediately whether it is the wrong data entry or whether patient is in the abnormal weight range.

Doctors are trained to record the history of present illness in narrative style especially for inpatients. Doctors may also prefer to record the current illness in text format. This implies that search facilities be included to extract the appropriate data from the structured format of the record system. Clinical narratives should be organised with the electronic record systems to facilitate the information retrieval. The electronic health record systems should not disrupt the workflow of the health care providers.

Data linkage and integration

As health information systems need to integrate among different healthcare institution 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 and message format standards organizations have developed standards for integration between them. 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 terminology development need to be incorporated to harmonise the standards.
There is, however, a potential for error from data integration. *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 (US Dept of Health and Human Services 1997).* Matching or integration of wrong patient would have serious effect on the person's health, research and public health. If the systems integrated use different units, different systems of measurement, data can be interpreted wrongly when it is integrated. Different unit and measurement such as 'Kg', 'lb', 'mg' and 'g' would make a difference in treatment and outcome. There may be different normal range for the laboratory results from one laboratory to another, and data could be interpreted wrongly after the integration. Different data standards could lead to interpret the data wrongly and that could harm the patient. Therefore unified standard of data is needed for the successful integration.

System Interoperability

The level of interoperability between systems should be in semantic operability so that information received could be interpreted as the same as the original message (NCVHS2000). If the interoperability is either basic or functional, there could be mistakes in interpreting the information transfer. Therefore systems developed need to follow data standards available. Abbreviation used should be uniform in different systems so that they could be interpretable in different systems. For example, PID, Pelvic Inflammatory Disease interpreted in one system should be the same in another system and not to be interpreted as the Pulmonary Infectious Disease. BPH, Benign Prostate Hypertrophy should be interpreted as the same in another system and not as the Blood Pressure High, URTI, Upper Respiratory Tract Infection should be interpreted the same and not as the Urinary Tract Infection. Data related to patient monitoring should be the same and should use the universal standards such as APGAR score for newborn so that it can be easily interpretable if the APGAR score is 7 or 10.

Integration of the different legacy systems is important to have easy accessibility and improve better decision making but at the same time, it should not impede the speed of the system. The system needs to maintain both the speed of searching and the completeness of the system. Different health information systems: laboratory system, pharmacy system, admission system, referral and discharge summary systems should be integrated, as also could be the separated subsystems so that the system would be specific to the specific healthcare providers.

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 the patient's allergy to a particular anesthesia

was not presented in a standard format and that was overlooked when the patient was prepared for the surgery (NCVHS200).

Security, Privacy and Confidentiality

Health data contains sensitive information of a person's health and compromising it could affect the person's life. To maintain the privacy and confidentiality of the system, the system needs to be secured. Security of the electronic health record systems may be implemented by physical system security , for example, providing authorised access to the user, by a firewall and by encryption technologies. It would be an intrusion of a patient's privacy if sensitive health information such as HIV status, obstetrics history and mental history was easily accessible, and it is necessary, therefore, to ensure that health information is disclosed only with the patient's consent except in emergency situations or for public health purposes.

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). Data users: healthcare providers and stakeholders have a duty to maintain the confidentiality of the data and systems developed need to deter access by unauthorized users. Users should abide by the law of privacy and legislation should be implemented according to the changing technology.
Healthcare providers also need to disclose confidential information where a failure to do so would constitute a threat to public or private interests, for example, reporting the communicable disease to the appropriate health organization. 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 the individual knows and understands the contents of the record. It is unethical to use implied consent when the patient is not fully aware of the information disclosure.

To protect a patient's privacy, each patient's EHR must be access- controlled. Each clinical record must be marked with a list of names accessible. And the level of access to various systems of the record can be controlled by the level of consent given by the patient.

Relationship framework for data quality and dependability of EHRs

Impaired data quality may 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 important roles in the data quality for the health information system. As stated previously, impaired data quality can have a direct impact on patient's health.

Figure 1 shows the relationship framework for dependability, data quality of the EHRs proposed for this study. Based on the literature review and this framework, checklist for the safety of the EHRs could be developed. System dependability will ensure the safety.

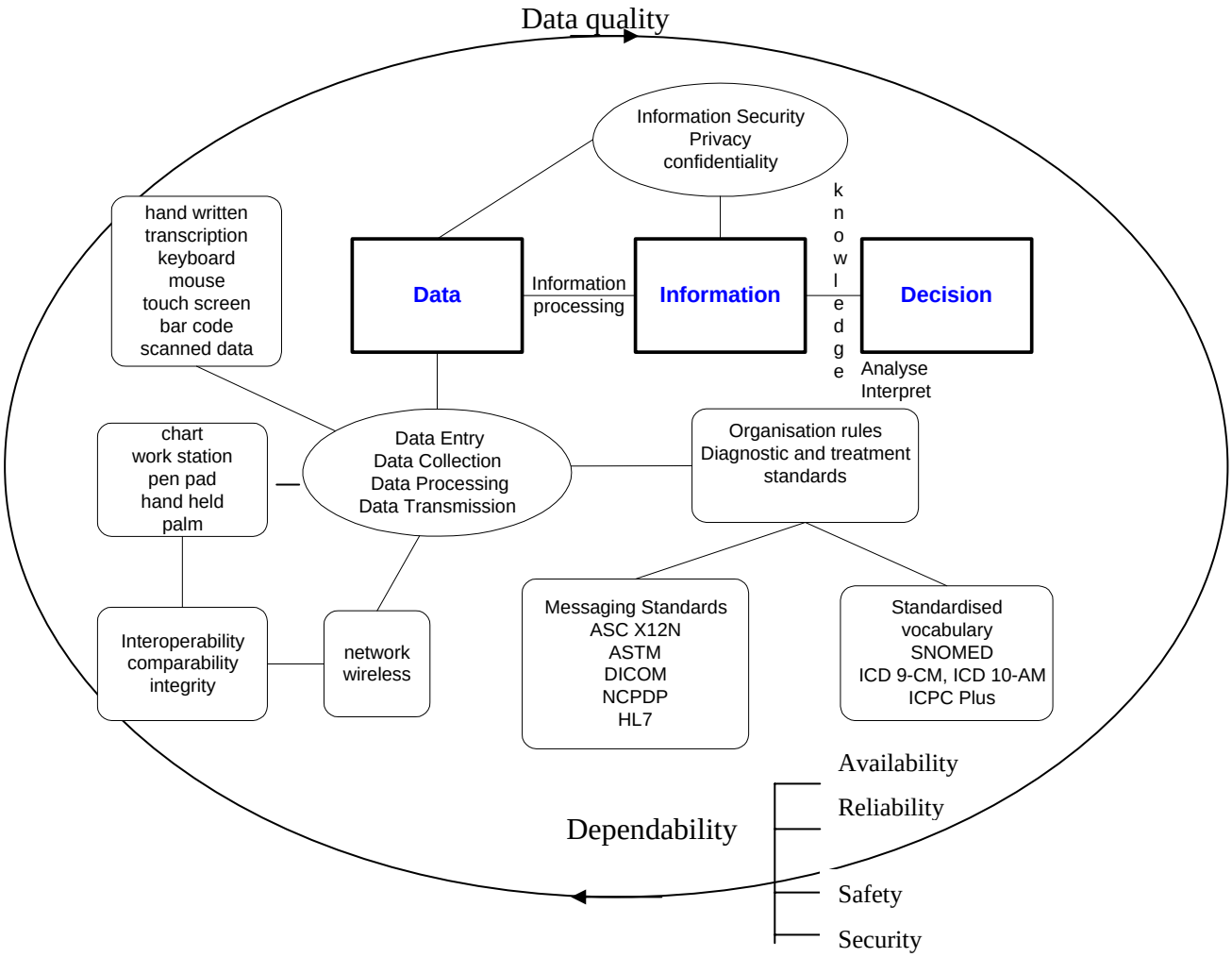

Figure 1: Relationship framework for data quality and dependability of EHRs

DEFINING THE SAFETY ATTRIBUTES OF EHRS

Based on the literature review and this framework, a checklist for the safety of the EHRs has been developed. As shown in figure 1, inappropriate data (Table 1) can occur in any steps involved in information processing: data entry, data collection, data processing and data transmission. Therefore, safety attributes for the EHRs are as shown in Table 3

There are different types of EHRs and safety assessment of the electronic health record systems needed to accommodate different EHR types. Table 3 outlines the checklist to identify safety of the EHRs.

Safety attributes of electronic health record systems
▪ 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
▪ 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
▪ data standards
▪ data interoperability
▪ data integrity
▪ attributes of data quality
1. availability
2. accuracy
3. completeness
▪ audit trail data
▪ disaster recovery
▪ storage
▪ back up
▪ retention period

Table 3 Safety attributes of electronic health record systems

The EHR system involves processes ranging from the data entry to information retrieval. To improve the safety of electronic health record, errors from the system need to be identified. As in all information systems, electronic health record systems include software, hardware and people. Determining the safety and performing risk assessment on the underlying technology and processes would reduce the causes of failure and improve the quality and safety of health care.

As discussed previously, there is documented evidence of medication errors. Lack of information about the patient and lack of knowledge of drugs strongly influence serious adverse drug events (Kuhn and Giuse 2001). To deter this, many health care institutions have started to implement computerised physician order entry systems (Murff and Kannry 2001; Ash et. al. 2003). Although these systems are implemented to improve patient safety, some systems have failed. An example would be the Cedar-Sinai Medical Centre, Computerised Physician Order Entry System where physicians petitioned to discontinue the system (Langberg 2003). The system was discontinued as there were concerns for safety and also it was disrupting the workflow.

4. Identifying the risk assessment method applicable to the EHRs

There are different risk assessment methods in software engineering. Some of the risk assessment techniques that can be used are:

- Root cause analysis, i.e., Fault tree analysis,

- Management oversight and risk tree analysis,
- Event tree analysis,
- Hazards and operability analysis,
- Failure Modes and Effects Analysis (FMEA), Failure Modes, Effects and Criticality analysis (FMECA) and
- Task and Human Errors analysis (Leveson 1995).

After careful consideration, some risk assessment methods were ruled out as they are not appropriate for EHRs. It was established in this research that fault tree analysis, event tree analysis and failure mode effect analysis were possible risk assessment methods for the EHRs.

a) Fault Tree Analysis:

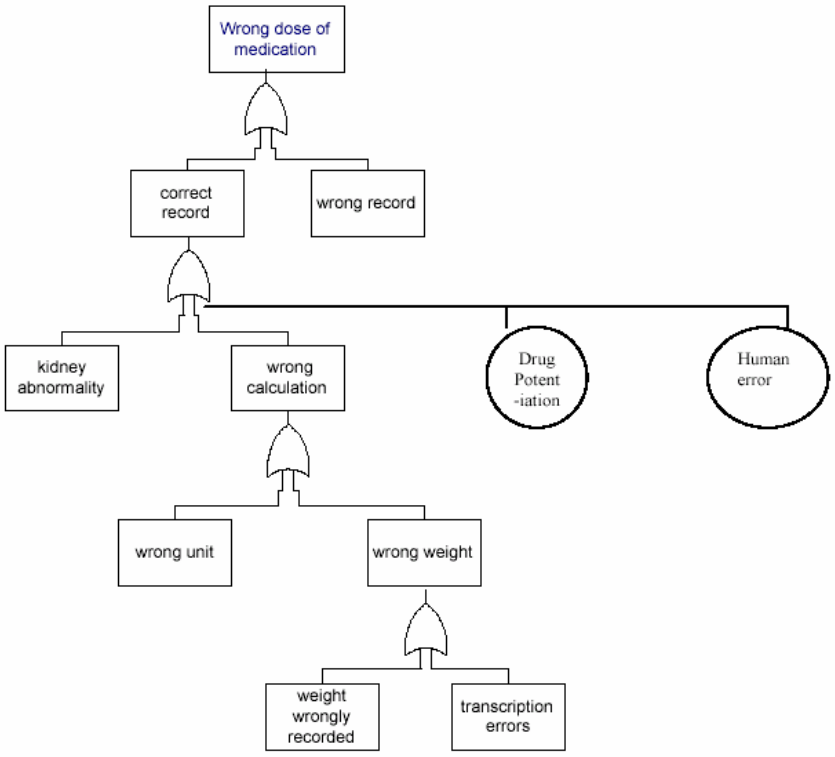

Figure 2: Fault Tree of Wrong dose of medication

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). Following example is the fault tree analysis for the wrong dose of medication. As seen in the example fault trees, the top event, adverse event wrong dose can be traced back to the bottom nodes.

b) Event Tree Analysis

This is a decision tree technique, which uses the 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 events leading up to it (Relex software corporation 2001). Figure 3 is an example of event tree analysis for failure for accessing the health record.

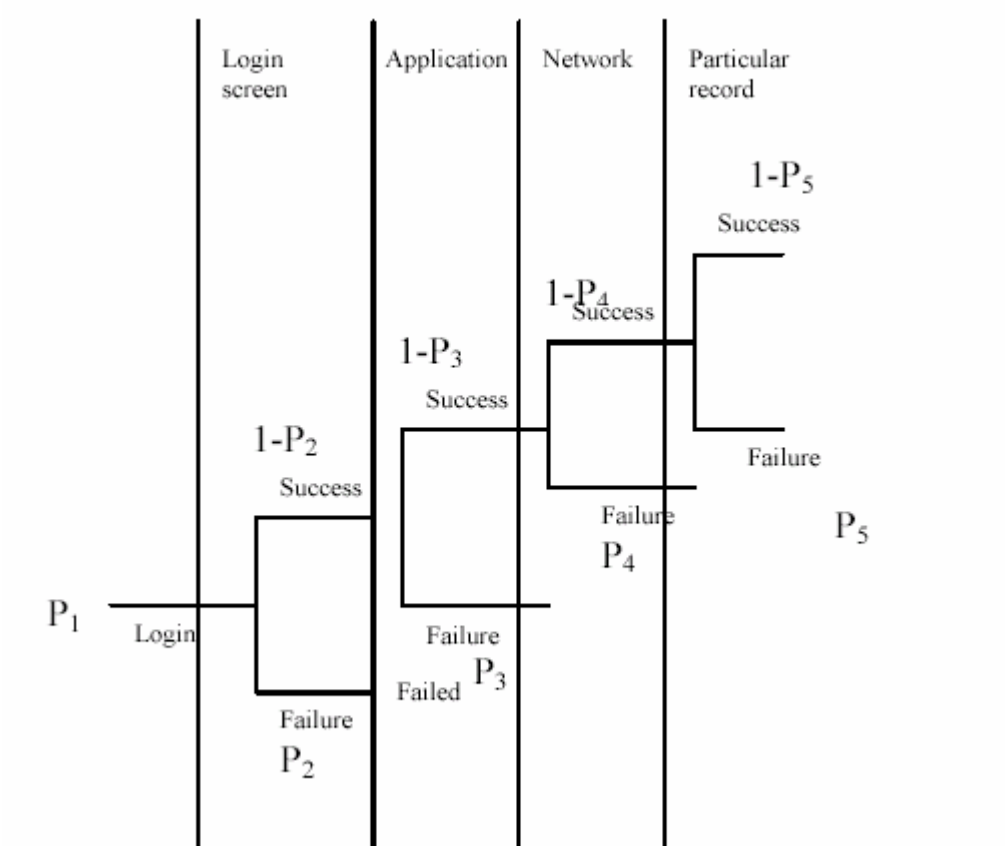

Figure 3: Event tree analysis for failure of access to health records

As demonstrated in Figure 3, the probability of accessing the record and failure can both be determined by the event tree. Failures can be from different states. It could be failure in the login screen, failure in application, failure in network, failure to access to the particular record. As shown in figure 3, probability of failure to login is P_2, the probability of successfully logging into the screen will be $1-P_2$. Likewise, if the probability of application failure is P_3 and the success would be $1-P_3$. Therefore, the probability of successful access to the particular record (P_x) can be calculated as

$P_x = P_1 (1-P_2) (1-P_3) (1-P_4) (1-P_5)$

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

c) Failure Modes and Effects Analysis (FMEA):

FMEA is a process for identifying the failure effects associated with individual failures within a system (Marx and Slonim 2003). It is necessary to identify whether FMEA could be applicable to the EHRs. To perform an FMEA, severity and probability of the potential failure mode needs to be identified. Hazard score is the multiplication of probability and severity. In this example, severity and Probability ratings are assigned values 1 to 4.

Severity Categories:	Probability ratings:
Catastrophic = 4 Major = 3 Moderate = 2 Minor =1	Frequent = 4 Occasional = 3 Uncommon = 2 Remote = 1

	Severity of Effect			
Probability	**Catastrophic**	**Major**	**Moderate**	**Minor**
Frequent	16	12	8	4
Occasional	12	9	6	3
Uncommon	8	6	4	2
Remote	4	3	2	1

Table 4: Hazard Scoring matrix

Electronic health record system involves processes ranging from data entry to decision making. For example, the outcome “wrong test result” can occur from errors in different steps in the process. The potential failure mode for each process can be identified as follows and risk assessment can be conducted through FMEA.

Figure 4 illustrates processes involved in the 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 4. Possible failure modes from these processes are shown in figure 6 to 8.

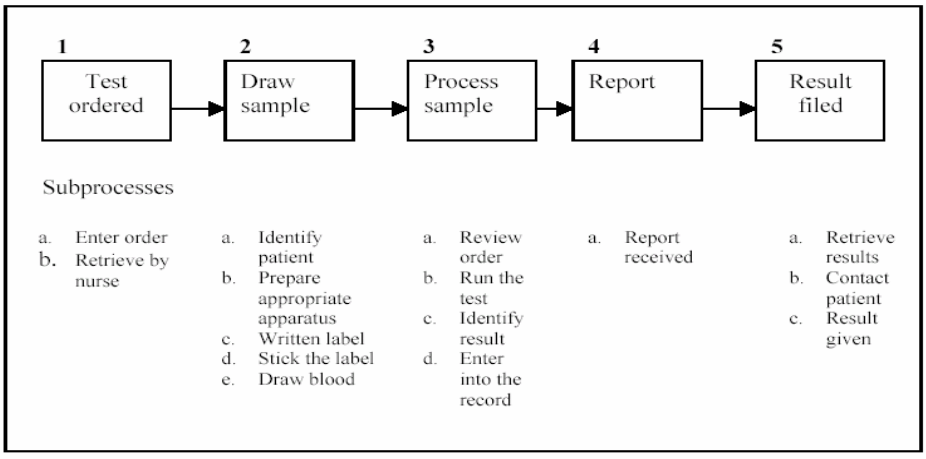

Figure 4: Processes involved in the laboratory test

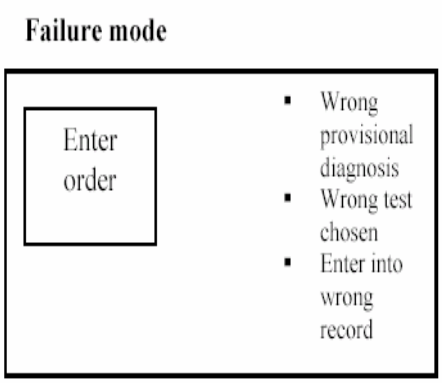

Figure 5: Failure mode for the process enter order

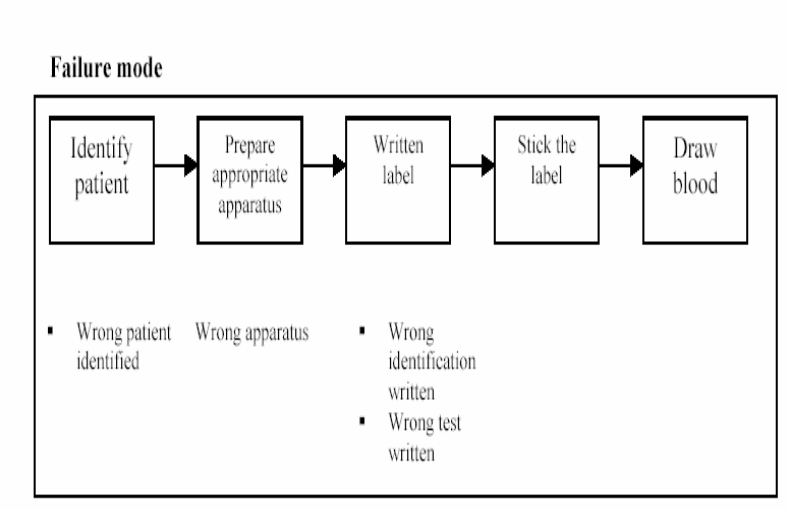

Figure 6: Failure mode for the process 2 (Draw Sample)

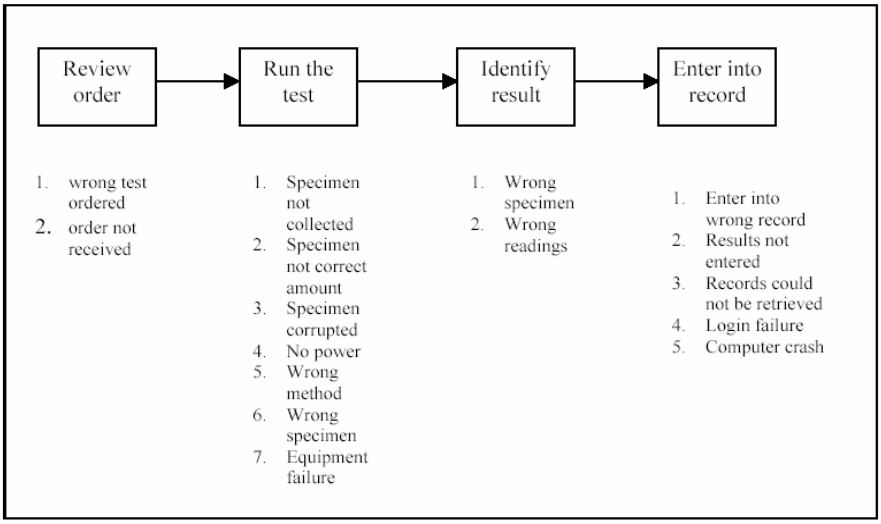

Figure 7: Failure mode for process 3 (Process Sample)

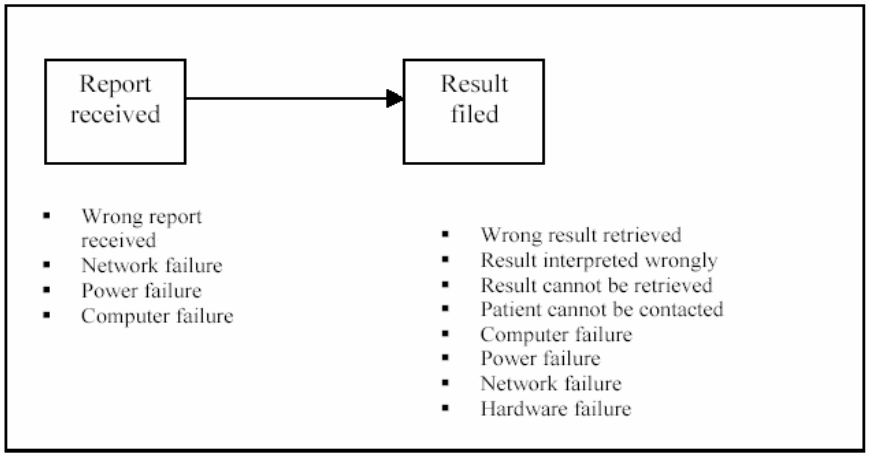

Figure 8: Failure mode for process 4 (Report) and 5 (Result filed)

As described above, we explored different risk assessment methods for the study and Failure Mode Effect Analysis was proposed as an appropriate method for the risk assessment of EHRs. Risk assessment conducting through FMEA involves identifying the possible failure modes of the system before the actual failure and that could mitigate the future occurrence of errors. Root cause analysis such as fault tree analysis is an alternative method of risk assessment but in fault tree analysis, the source of error is identified after the incident happened. Therefore, fault tree analysis is suitable for retrospective studies, where adverse events or errors have occurred and to track back the root cause conditions. With FMEA, failure mode will be predicted first and could prevent the condition from occurring. It is important to identify the possible risk first to ensure the safety. Therefore, FMEA was selected as the most suitable risk assessment method for EHRs.

CONCLUSION

This paper highlights the importance of safety of EHRs. Key safety attributes were identified in the EHR context. Based on this research, it can be concluded that identifying the relationship between data quality and dependability is important for EHRs, as this enables the identification of essential attributes of EHRs. This research also identifies the appropriate risk assessment methods for EHRs. Conducting risk assessment method of EHRs would highlight the potential risk. If potential risks are identified, these can be mitigated or reduced and this will enhance safety.
Safety attributes of EHRs identified by this research will be valuable for future EHRs implementation. Thorough research indicated that there is no identified risk assessment method for EHR currently. It is suggested that the proposed risk assessment method for EHRs will be invaluable for EHRs around the world.

REFERENCES:

Ash J. S., Gorman P. N., Seshadri V., and. Hersh W. R.(2003), “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

Davis P., Lay-Yee R., Briant R., Schug S., Scott A. ,Johnson S.(2001), 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

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

Healthcare Failure Mode and Effect Analysis Course Materials (2003), VA National Center for Patient Safety, available at http://www.patientsafety.gov/HFMEA.html

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

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

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/

Kaushal R. and Bates D. W. (2002), "Information Technology and medication safety: what is the benefit?", **Quality and safety in health care**, vol. 11, pp. 261-265

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

Leveson N. G. (1995), **Safeware: System Safety and Computers**, Addison-Wesley.

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

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

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

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

Relex Software Corporation (2001), **Visual Reliability Software**, available at www.fault-tree.com accessed November 2001

Sommerville I (2001), **Software Engineering**, sixth edition, Addison Wesley, ISBN 0 201 39815 X

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

Weingart S. N., Wilson R. M., Gibberd R. W., Harrison B. (2000), “Epidemiology of medical error”, **British Medical Journal**, vol. 320, pp 774-777

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.