

Electronic health record system risk assessment: a case study from the MINET

Khin Than Win, Hai Phung, Lis Young, Mai Tran, Carole Alcock, Ken Hillman

Abstract

This article discusses the risk assessment of a health information system. A case study was conducted at the South Western Sydney Area Health Service to examine the potential risks of the Maternal and Infant Network (MINET) health information system using Failure Mode Effect Analysis (FMEA). FMEA was conducted by utilising safety attributes identified by the authors. Potential failure modes of the system were identified by the study. From this study, it can be concluded that FMEA is an appropriate risk-assessment method for MINET.

Keywords: *Health information; risk-assessment; safety.*

Introduction

A thorough literature search indicates that there has been little study to date on risk-assessment methods for electronic health record systems. Although there have been assessments of project management and security risk to systems, there has been no safety risk assessment. The main objective of this study was to identify possible risks in a health information system (the Maternal and Infant Network: MINET) using Failure Mode Effect Analysis (FMEA). In particular, this article describes a risk-assessment case study conducted at the Simpson Centre for Health Services Research. Identifying possible failures from the system could mitigate or prevent its potential failure, while also enhancing the safety of the system.

Background

The report *To err is human: building a safer health system* (Kohn et al. 2000) emphasised the importance of safety in healthcare. 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 number of lives lost to preventable medication errors alone represents over 7000 deaths annually, which is more than the number of injuries in US work places (Institute of Medicine 2000). The 1998 National Survey of New Zealand has documented that 4.5% of all hospital 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).

As electronic health record systems are part of the overall healthcare system, it is important to ensure that electronic health data are secure and dependable in order to reduce the risk of occurrence of medical errors. The identification of safety requirements of electronic health record systems would also help to reduce errors (Win et al. 2002). Exploring undesirable events that can occur from electronic health record systems would assist in identifying risk.

There are specific risk-assessment methods available for different systems. With proper risk assessment, potential risks can be identified and avoided, resulting in a safer health record system, and ultimately

1: Safety attributes of EHRs

- 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

mately in safer healthcare. Awareness of risk and safety requirements is important, as it will assist in re-engineering of the appropriate electronic health record systems for healthcare organisations.

Safety and dependability

Drawing on the relationship framework for dependability and data quality and the literature review under-

2: Relationship of data quality and dependability

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

taken, we have identified safety attributes for Electronic Health Records (EHRs). However, as EHRs can have different purposes for different information management and systems, safety attributes may also differ (Schloeffel & Jeselon 2002; Shiffman et al. 1999). Attributes of dependability include availability, reliability, security and safety (Sommerville 2001).

Data quality

Data quality has been 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). Whenever possible, data quality should not be compromised, because low quality health data will have a significant impact on decision-making processes on information management.

Data quality and dependability

Box 2 presents characteristics involved in healthcare data quality. It shows how data quality is related to the dependability and lists appropriate measures needed to ensure data quality.

Electronic Health Record Systems (EHRs)

A Health Information Network for Australia identified the electronic health record as:

... 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 (A Health Information Network for Australia, 2000).

Humphreys has defined health records which are used in health services research for monitoring public health and outcomes as ‘population health records’ (Humphreys 2000). However, these records are also used for data acquisition, record keeping, communication, integration, surveillance, information storage and retrieval, and data analysis. These attributes also apply to EHRs, as defined by Perreault and Wiederhold (1990); therefore, MINET can be categorised as one of the EHRs.

MINET case study

The case study was conducted at the Simpson Centre for Health Services Research, from the Maternal and

Infant Network (MINET) database. MINET was selected as a case study for this research as it involves different electronic health data from different sources. The MINET database contains health data on infants and children in the South Western Sydney Area Health Service (SWSAHS) from the prenatal period to school age (0-5 years). MINET involves community-based data from the Ingleburn Baby Information System (IBIS Database) and obstetric and gynaecological data (OBSTET) from the hospital data system. MINET caters for all persons living in the SWSAHS. These data are important for public health and health service research, because the prenatal and infant and early childhood periods are critical for the promotion of good health and the development of personal characteristics for adolescence and adulthood (Halldorsson et al. 1999). It is also important that the databases are accurate for the purposes of health service research. As part of MINET, OBSTET data are downloaded to the Simpson Centre for Health Data Research only and Simpson Centre does not have any control over how the OBSTET data are collected and processed.

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 for IBIS: baseline and follow-up data. The IBIS baseline form is used for the first visit at the baby clinic and the IBIS follow-up form is used for subsequent visits.

Methodology

Different methods have been explored in order to identify one that is appropriate for risk assessment of EHRs. Failure Mode Effect Analysis (FMEA) was proposed because risk assessment conducted through this method involves identifying the possible failure modes of the system before failure can occur (Win, Cooper & Alcock 2004). An alternative method of risk assessment is root cause analysis, for example fault-tree analysis; however, this method identifies the source of error after the event. Fault-tree analysis is more suitable for retrospective studies of systems in which adverse events or errors have already occurred, or to track back to the root-cause conditions. With FMEA, failure mode can be predicted and action taken to prevent the condition from occurring in the first place (Win 2004). It is clearly important to identify any possible risks first to ensure the system’s safety, so FMEA is a more suitable approach compared with root-cause analysis in this case.

Failure Mode Effect Analysis (FMEA)

Failure Mode Effect Analysis is a structured approach to the prediction and identification of the consequences of failures in a system. To conduct an FMEA, the processes involved in the system can be subdivided into sub-processes and possible failure modes of these processes. Upon identification, their potential effects can be estimated and analysed to prevent the possible failures.

3: Level of probability

Probability

- Low: rarely or never occurs
- Medium: occurs occasionally or few times per year
- High: occurs regularly or weekly basis

4: Level of severity

Probability

- Low: rarely or never occurs
- Medium: occurs occasionally or few times per year
- High: occurs regularly or weekly basis

5: Risk/hazard score

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

To conduct risk assessment of MINET using FMEA, severity and probability of identified risks need to be determined. Definition of severity and probability level are presented in Boxes 3 and 4. Risk or hazard score can then be determined. This is shown in Box 5.

Processes involved in the MINET database are described in Box 6.

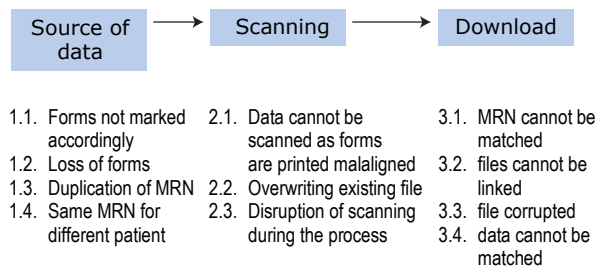
6: Processes involved in MINET database

1. **Source of data** Face to Fill in the form (IBIS)
face data
collection
2. **Scanning** From form into the text file using the scan software
3. **Download** From text file to access database using Microsoft Access

Results and discussion

Possible failure modes of MINET can be predicted as illustrated in Box 7.

7: Possible failure modes from processes



Potential effects, severity, probability and hazard score of each potential failure mode are described in Box 8.

These identified hazards were notified to the authorised personnel responsible for the system and necessary actions were identified.

The following section presents the analysis of possible failure modes identified in Box 7. These include *Forms not marked appropriately* and *Missing forms*. Forms that are not marked appropriately could be ruled out at the time of the scanning process. This can be due to human error, and the Simpson Centre needs to trace them back to the Community Health Centre. Patients' data are filled in manually at the Community Health Centres and compiled to scan.

Duplication of MRNs and *Same MRN for different patients* are also possible failures in the source of the data, as identified in Box 7. It is noted that different medical record numbers (MRNs) are used in different services. In addition, maternal and infant MRNs can differ, leading to the possibility of incorrect association of maternal and infant MRNs; for example, parents may be unmarried, or a mother might not necessarily change her surname upon marriage, in which case the mother's and infant's surnames will be different. In some cases, a mother's surname could be changed from the previous childbirth history as a result of subsequent marriage or divorce. Duplication of MRNs for the same person at different services or at the same service is always a possibility, and several problems could result from wrong linkage of the data. Data may be linked to the wrong patient at the time of analysis and there can be errors in predicting health indicators.

Possible failure modes during scanning and downloads have been identified in Box 7. Scanning is done in batch processing, and some documents could be misplaced and lost during this process. To avoid this problem, it is advisable to have computerised data entry at the point of care.

Files cannot be linked if the system is unavailable due to such factors as power loss or application failure. The centre has not yet experienced application failure, and, as it is not a 'real time' system, power loss for a limited period is acceptable. There would also be loss of data should the data file be corrupted, and the Simpson Centre regularly backs up data so that this can be prevented. There is also a high probability that data from different databases cannot be matched properly, as different versions of IBIS have different data units. These problems need to be addressed at the time of form download and during statistical analysis.

Wrong data linkage can lead to incomplete and inaccurate data, and in the case of clinical data this could result in a significant and immediate impact on the patient. The Simpson Centre uses aggregated data for statistical analysis, and records not matched perfectly are excluded from the analysis. Disruption may occur in the scanning process due to mechanical problems with the machine, power failure, or inexperienced scanning operators. When detected during the scanning process, the problem can be rectified to minimise impact on the system; the only impact would then be on the scanning task the person was performing at the time.

The focus of the Simpson Centre database MINET is on maternal and child health. The IBIS manual clearly explains the format of questions, why the data are collected, what the data are about and standards for completion. IBIS data have been considered for completeness, legibility and integrity of information. Data are gathered with clear understanding of future uses.

Box 8 illustrates the FMEA of different processes. With FMEA, possible failure modes have been identified and predicted for different processes involved in MINET. However, as security of health data is important because it contains sensitive information relating to a person's health, risks regarding security, privacy and confidentiality of the system need to be explored. These failure modes are identified in 4.1 and 4.2 of Box 8.

Security, privacy and confidentiality

Security of EHRs could be implemented through the physical security of the system; for example, by providing authorised access only to the user, and by application of firewall and encryption technologies. Assessment of MINET's information security and vulnerability to threats indicates that, because the system is located in the Intranet, anti-virus software was installed on all servers, desktop and laptop computers, and there are both internal and external firewalls to protect information. In addition, there is an audit trail configured to log all transactions. Log file analysis is carried out daily and reports of unusual, inappropriate or anomalous activities are sent to the system administrator. The system guards against unscrupulous attack to the system.

MINET ensures the confidentiality and privacy of the health data: each patient consents to disclose their information for research purposes; there is an authenticated log-in to the system; there is a policy regarding access; and there is a list of users who could access the system. User access level is predetermined and only authorised users can access the system. Access control is available for system usage and user responsibilities; a user group for MINET determines the access levels. The system provides a password management function to allow password changes to be announced. Individuals have their own passwords, and it is not possible to eavesdrop upon account authentication. To avoid breach of confidentiality, and because it is difficult to trace, guest or anonymous log-in is not allowed. Passwords include a combination of alphabetic, numeric and special characters. A first-time password is transmitted securely.

MINET is a distributed system, and data files and the database are stored on the server. Back-up is performed at the Simpson Centre and the other community health service centres. Back-ups are stored securely under lock and key, and the Information Service Department has data back-ups on tapes, while the Simpson Centre has data back-ups on hard disks. The Simpson Centre uses de-identified data for research purposes, thus maintaining patient confidentiality. The Centre follows the *Database and data extracts policy and guidelines* from the South Western Sydney Area Health Service.

8: Failure mode effect analysis of different processes

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 MRN for the same person	Data unavailable or misleading data for the research purpose	Medium	Medium	4
1.4. Same MRN for different patient	Misleading data for the research purpose	High	Medium	6
2.1. Forms are printed malaligned	Documents unscannable	Low	Low	1
2.2. Overwriting 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
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

Conclusion

The Simpson Centre uses data mainly for health services research, an important role, as it could affect public health research in, for example, healthcare processes, disease patterns, disease surveillance, prevention of disease and health promotion. Data from MINET are used for health services research, and conducting a risk assessment study has had a positive effect, as inaccurate or incomplete information can have an impact on health outcome indicators. It is very important that electronic health data from MINET are complete and accurate, as MINET is used for data collection, analysis and interpretation of data for early intervention, planning, prevention and evaluation.

Although MINET data are health data, it can be seen that not all safety attributes identified are appropriate for this system. As MINET is aggregated data and it is used for de-identified data, the requirement that a patient’s name and identification be displayed on every screen is not applicable to MINET. However, it can be concluded that unique patient identification is very important for MINET, as there could be different potential effects (as described above) if a patient could not be uniquely identified. Alerts and reminders could assist in follow-up and referral for community health, but they do not have a significant impact on the health service research data for MINET. They could, however, be appropriate for disease surveillance health research in different aggregated data sets. Data regarding medication and dosage could be important for mater-

nal and child health data in community care; for example, errors in a child’s medication dosage could result in a serious outcome. Including information regarding these data will add value to the system.

As for all health informatics systems, issues of privacy, confidentiality and security are important in MINET. Those involved with data entry and processing are given a clear explanation of privacy policy and are therefore aware of confidentiality concerns. Access level is decided by the user group, and the administrator needs to set the level accordingly to ensure the privacy of data.

As data from a number of sources are used for research, common standards are important for different databases. Completeness of data is essential for MINET databases, as incomplete data will result in errors in statistical analysis, which will in turn have an impact on healthcare indicators. FMEA has identified possible failures of the system and is therefore an appropriate risk-assessment method for the MINET.

Acknowledgements

The authors would like to thank the staff of the Simpson Centre, especially Monica Alberto and the community-based and hospital-based staff from SWSAHS, for their efforts in the collection and maintenance of the MINET database. The authors also acknowledge the contribution of all staff working in the area of maternal and child health continuum of care in SWSAHS.

References

- National Electronic Health Record Taskforce (2000). *A Health Information Network for Australia*. Report to Health Ministers by the National Electronic Health Record Taskforce. Commonwealth of Australia. Available at: http://www.health.gov.au/healthonline/ehr_rep.pdf (Accessed October 2000).
- Arts, D.G.T., Keizer, N.F.D. and Scheffer, G-J. (2002). Defining and improving data quality in medical registries: A literature review, case study, and generic framework. *Journal of the American Medical Informatics Association* 9: 600-611.
- Davis, P., Lay-Yee, R., Briant, R., Schug, S., Scott, A., Johnson, S. and Bingley, W. (2001). *Adverse events in New Zealand public hospitals: principal findings from a National Survey*. Occasional paper, December 2001. Wellington, New Zealand, Ministry of Health.
- Halldorsson, M., Cavelaars, A.E., Khnst, A.E. and Mackenbach, J.P. (1999). Socioeconomic differences in health and well-being of children and adolescents in Iceland. *Scandinavian Journal of Public Health* 27: 43-47.
- Humphreys, B.L. (2000). Electronic health record meets digital library: a new environment for achieving an old goal. *Journal of the American Medical Informatics Association* 7(5): 444-452.
- 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. Available at: <http://www.quic.gov/report/mederr2.htm>
- Kohn, L.T., Corrigan, J.M., Donaldson, M.S. (2000). *To err is Human: building a safer health system*. Washington D.C., National Academy Press.
- Perreault, L.E. and Wiederhold, G. (1990). System Design and Evaluation. In: *Medical informatics: computer applications in health care*. E.H. Shortliffe and L.E. Perreault (Eds). Reading, Mass., Addison-Wesley.
- Schiffman, R.N., Brandt, C.A., Liaw, Y. and Corb, G.J. (1999). A design model for computer based guideline implementation based on information management services. *Journal of the American Medical Informatics Association* 6(2): 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/ISO_HER_FinalReport.pdf (Accessed 22nd April 2003).
- Sommerville, I. (2001). *Software engineering* (Sixth edition). Reading, Mass., Addison-Wesley.
- Weingart, S.N., Wilson, R.M., Gibberd, R.W. and Harrison, B. (2000). Epidemiology of medical error. *British Medical Journal* 320: 774-777.
- Win, K.T., Croll, P. and Cooper, J. (2002). Setting safety standards for electronic medical records. *Proceedings of HIC2002, The Tenth Annual Health Informatics Conference*, Melbourne, August 4-6.
- Win, K.T., Croll, P. and Cooper, J. (2003). Dependability: important factor for the success of electronic health record

systems. *Proceedings of the Eleventh Annual Health Informatics Conference*, Sydney, August 10-12.

Win, K.T., Cooper, J. and Alcock, C. (2004). Risk assessment of electronic health record systems. *Proceedings of COLLECTeR 2004, the Twelfth COLLECTeR Workshop on eCommerce*, Adelaide, May 7-8.

Win, K.T. (2004). Identifying the risk assessment method applicable to the electronic health record systems. *Proceedings of the Twelfth National Health Informatics Conference HIC2004*, Brisbane, July 25-27.

Khin Than Win

Lecturer
School of IT and Computer Science
Faculty of Informatics
University of Wollongong
Email: win@uow.edu.au

Khin Than Win is a Lecturer at the School of Information Technology and Computer Science, University of Wollongong, Australia. She is a medical doctor with a postgraduate degree in Computer Information Systems. She is pursuing a PhD in Health Informatics. Her research interests are in issues related to electronic health record systems. She teaches Health Informatics subjects to undergraduate and postgraduate students. She is also supervising several honours and postgraduate research students in health informatics.

Hai Phung

The Simpson Centre For Health Services Research,
Liverpool Hospital
Faculty of Medicine, The University of New South Wales

Lis Young

The Simpson Centre For Health Services Research,
Liverpool Hospital
Faculty of Medicine, The University of New South Wales

Mai Tran

The Simpson Centre For Health Services Research,
Liverpool Hospital

Carole Alcock

Faculty of Informatics, University of Wollongong

Ken Hillman

The Simpson Centre For Health Services Research,
Liverpool Hospital
Faculty of Medicine, The University of New South Wales