IMPLEMENTATION OF REQUIREMENTS ENGINEERING METHOD ON HANDLING PATIENT DATA

ZURAIN BINTI NASARUDDIN @ ISMAIL SHAH

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Science (Information Security)

School of Computing
Faculty Engineering
Universiti Teknologi Malaysia

AUGUST 2018

This project report is dedicated to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

Alhamdulillah. Thanks to Allah SWT, whom with His willing to give the opportunity to me to finish the project entitled 'Implementation of Requirements Engineering Method on Handling Patient Data'. Firstly, I would like to express my deepest thanks to **Dr. Siti Hajar Othman** as a supervisor who had been guided me during this project.

Also thanks to the respondents from the Klang hospital for giving cooperation during the data collection process. I also want to thanks the lecturers of Faculty of Computing, UTM for their valuable information, suggestions and guidance in the preparation and compilation of this project report.

A deepest thanks and appreciations to my beloved parents and siblings for their encouragements, cooperation, constructive suggestions and full of support for the project completion from the beginning until the end.

In addition, thanks to all my dearest friends who has been contributed by supporting and helping me during the project progress. Last but not least, thanks to everyone who involved directly and indirectly either advice, opinion, criticizes, knowledge or helping hands. Thank you.

ABSTRACT

A personal data is information which relate to a person or individual who can be identified from those data. These information is an important resource and asset to any organization especially in healthcare system. The healthcare system data has a high level of privacy as it may contain the sensitive data as well, thus, there is a need to have personal data protection in the healthcare system. To ensure there is a personal data protection, an assessment on the personal data security has to be done. This project is adapting a requirements engineering method and addressing the problems related to the personal data security regarding patient records. The requirements engineering follows the contents of the Simple Reuse of Requirements (SIREN). There are a total of five processes in the requirements engineering method for healthcare. The requirements listed through the requirements engineering process are obtained through the personal data activities such as collection, use, disclosure, security and retention of personal data. The sources in Malaysia healthcare system includes the laws and standards enacted which are confidentiality guidelines and Personal Data Protection Act in Malaysia are followed. The survey conducted in Klang hospital showed that almost all requirements are followed, thus, it can be concluded that confidentiality of patient data in Klang hospital are assured.

ABSTRAK

Data peribadi adalah maklumat yang berkaitan dengan seseorang atau individu yang boleh dikenal pasti daripada data tersebut. Maklumat-maklumat ini merupakan sumber dan aset yang penting kepada mana-mana organisasi terutama dalam sistem penjagaan kesihatan. Data sistem penjagaan kesihatan mempunyai tahap privasi yang tinggi kerana sistem juga mungkin mengandungi data sensitif. Oleh itu, perlindungan data peribadi dalam sistem penjagaan kesihatan adalah diperlukan. Untuk memastikan adanya perlindungan data peribadi, penilaian pada jaminan data peribadi perlu dilakukan. Projek ini menyesuaikan kaedah kejuruteraan keperluan dan menangani masalah-masalah yang berkaitan dengan jaminan data peribadi mengenai rekod pesakit. Kaedah kejuruteraan keperluan mengikuti kandungan guna semula keperluan. Terdapat lima proses dalam kaedah kejuruteraan keperluan untuk penjagaan kesihatan. Keperluan yang disenaraikan melalui proses kejuruteraan keperluan diperolehi melalui aktiviti data peribadi seperti pengumpulan, penggunaan, penzahiran, keselamatan dan pengekalan data peribadi. Sumber-sumber dalam sistem penjagaan kesihatan Malaysia yang perlu diikuti termasuklah undang-undang dan piawaian yang digubal iaitu garis panduan sulit dan rahsia dan juga Akta Perlindungan Data Peribadi di Malaysia. Kaji selidik yang telah dijalankan di Hospital Klang menunjukkan bahawa perlindungan data pesakit di hospital tersebut terjamin.

TABLE OF CONTENT

CHAPTER	TITLE		PAGE
	ACKNOWLEDGEMENT		**iv**
	ABSTRACT		**v**
	ABSTRAK		**vi**
	TABLE OF CONTENT		**vii**
	LIST OF TABLES		**xii**
	LIST OF FIGURES		**xiv**
	LIST OF APPENDICES		**xvi**
1	**INTRODUCTION**		**1**
	1.1	Introduction	1
	1.2	Problem Background	3
	1.3	Problem Statement	4
	1.4	Project Research Aim	5
	1.5	Objectives	5
	1.6	Research Scope	6
	1.7	Research Contribution	6
	1.8	Report Organization	7
2	**LITERATURE REVIEW**		**8**
	2.1	Overview	8
	2.2	Personal Data Security	9
		2.2.1 Privacy	9
		2.2.2 Personal Data	10

	2.2.3	Personal Data in Medical or Health System	11
	2.2.4	Personal Data Protection	13
2.3	Personal Data Security Assessment Methods		14
	2.3.1	Approach 1: Data Protection Audit	14
	2.3.2	Approach 2: Privacy Audit Methodology	17
	2.3.3	Approach 3: Audit Recommendation for Privacy Protection	19
	2.3.4	Approach 4: Audit Guideline for Vulnerability Analysis	20
	2.3.5	Approach 5: Clinical Audit Cycle	21
	2.3.6	Approach 6: E-health Internationalization Requirements	23
	2.3.7	Approach 7: Personal Data Audit through Requirements Engineering	26
	2.3.8	Comparison on Approaches of Personal Data Audit	28
	2.3.9	Selected Approach	31
		2.3.9.1 PDA-RE	31
2.4	Requirements Engineering		33
	2.4.1	Requirements Engineering in Engineering Field	34
	2.4.2	Requirements Engineering in Education System	35
	2.4.3	Requirements Engineering in Financial	36
	2.4.4	Requirements Engineering in Legal and Law-Related	37
	2.4.5	Table of Comparison on Requirements Engineering	38
	2.4.6	Requirements Engineering in Medical or Health System	39

	2.5	Assessment on Personal Data Security through Requirements Engineering for Public Hospital in Malaysia		40
		2.5.1	Healthcare in Malaysia	40
			2.5.1.1 Public Hospital in Malaysia	41
			2.5.1.2 Security Policy in Klang Hospital	42
		2.5.2	Requirements Engineering References on Healthcare in Malaysia	42
			2.5.2.1 Confidentiality Guidelines	43
			2.5.2.2 Personal Data Protection Act	44
	2.6	Chapter Summary		46
3	**RESEARCH METHODOLOGY**			**47**
	3.1	Overview		47
	3.2	Research Framework		48
		3.2.1	Phase 1: Planning	49
		3.2.2	Phase 2: Implementing	49
		3.2.3	Phase 3: Evaluating	50
	3.3	Project Deliverables		51
	3.4	Project Requirements		53
	3.5	Project Work Plan		54
	3.6	Chapter Summary		54
4	**RESEARCH DESIGN AND IMPLEMENTATION**			**55**
	4.1	Introduction		55
	4.2	Research Gap		56
	4.3	Initial Development		56
	4.4	Finalize Framework		57

		4.4.1	Processes of Requirements Engineering Method	58
			4.4.1.1 Step 1: Definitions of Systems Goals	59
			4.4.1.2 Step 2: Requirements Elicitation	60
			4.4.1.3 Step 3: Requirements Analysis	63
			4.4.1.4 Step 4: Requirements Specification	64
			4.4.1.5 Step 5: Requirements Validation	64
	4.5	Questionnaire Development		65
	4.6	Data Collection		66
	4.7	Chapter Summary		67
5	**FINDINGS AND ANALYSIS**			**68**
	5.1	Introduction		68
	5.2	Questionnaire Analysis		69
		5.2.1	Section A: General	69
		5.2.2	Section B: Personal Data Protection Act (PDPA) 2010	76
		5.2.3	Section C: Confidentiality Guidelines by Malaysia Medical Council (MMC)	78
		5.2.4	Section D: Requirements	88
	5.3	Requirements Engineering		88
		5.3.1	Requirements Analysis	89
		5.3.2	Requirements Specification	91
		5.3.3	Requirements Validation	93
	5.4	Expert Review and Justification on the Structure		96
	5.5	Chapter Summary		97

6	**CONCLUSION**		**98**
	6.1	Introduction	98
	6.2	Overview of study	98
	6.3	Limitation of the Project	99
	6.4	Future recommendation	99
	6.5	Project Achievement	100
	6.6	Concluding Remarks	100
	REFERENCES		**102**
	APPENDICES		**105**

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Table of Comparison on Approaches of Personal Data Assessment	29
2.2	Table of Comparison on Requirements Engineering	38
3.1	Research Phases	48
3.2	Project Deliverables	52
4.1	List of Requirements	61
4.2	Nominal Scale	66
5.1	Demographic Variable and Measure	69
5.2	Demographic of Gender	70
5.3	Demographic of Age	71
5.4	Demographic of Education	71
5.5	Job Type	72
5.6	Job Experience	73
5.7	Understanding on PDPA	74
5.8	Understanding on Confidentiality Guidelines	74
5.9	Understanding on Requirements Engineering	75
5.10	PDPA Q1 to Q7	77
5.11	PDPA Q8	78
5.12	Principles on Confidentiality Guidelines	79
5.13	Protecting Information	79
5.14	Disclosures Required by Law	80
5.15	Disclosures with Consent	81
5.16	The Patient's Interest	82
5.17	The Public Interest	82

5.18	Disclosures about Patients who Lack Capacity to Consent	83
5.19	Sharing Information with a Patient's Spouse, Partner, Carers, Relatives or Friends	84
5.20	Genetic and Other Shared Information	85
5.21	Disclosure after a Patient's Death	85
5.22	Media Inquiries about Patients	86
5.23	Responses for all Parts of Confidentiality Guidelines	87
5.24	Feedback on Requirements	89
5.25	Total Responses on Requirements Questions	91
5.26	Requirements Specification	91
5.27	Total Specification Requirements	93
5.28	Validation of Software Specification Requirements	93
5.29	Total Validation of Software Specification Requirements	94
5.30	Validation of System Specification Requirements	94
5.31	Total Validation of System Specification Requirements	96
5.32	Expert Reviews	96

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
2.1	Personal Information	10
2.2	Data Protection Audit Program	15
2.3	Plan-Do-Check-Act Cycle	16
2.4	Chain of Audit Process	16
2.5	Privacy Audit Methodology Structure	18
2.6	An Overview of the Audit Recommendation Framework	19
2.7	Process Flow for Security Audit	21
2.8	Clinical Audit Cycle	22
2.9	Internationalization Requirements Catalogue Generation Process	24
2.10	e-Health Internationalization Audit Method	25
2.11	Sources of SIREN PDP Catalogue Contents	26
2.12	Phases of the Personal Data Audit Method	32
3.1	Research Framework	50
4.1	Requirements Engineering Structure of Personal Data Security on Healthcare-Based	57
5.1	Statistics Graph of Gender	70
5.2	Statistics Graph of Age	71
5.3	Statistics Graph of Education	72
5.4	Statistics Graph of Job Type	72
5.5	Graph of Job Experience	73
5.6	Graph of Understanding on PDPA	74
5.7	Graph of Understanding on Confidentiality Guidelines	75
5.8	Graph of Understanding on Requirements Engineering	76

5.9	Graph of PDPA Q1 to Q7	77
5.10	Graph of PDPA Q8	78
5.11	Graph of Principles on Confidentiality Guidelines	79
5.12	Graph on Protecting Information	80
5.13	Graph on Disclosures Required by Law	80
5.14	Graph on Disclosures with Consent	81
5.15	Graph on the Patient's Interest	82
5.16	Graph on the Public Interest	83
5.17	Graph on Disclosures about Patients who Lack Capacity to Consent	83
5.18	Graph on Sharing Information with a Patient's Spouse, Partner, Carers, Relatives or Friends	84
5.19	Graph on Genetic and Other Shared Information	85
5.20	Graph on Disclosures after a Patient's Death	86
5.21	Graph on Media Inquiries about Patients	86
5.22	Graph on Responses for all Parts of Confidentiality Guidelines	87

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
APPENDIX A: Gantt Chart Project 1		106
APPENDIX B: Gantt Chart Project 2		108
APPENDIX C: Survey Form		110

CHAPTER 1

INTRODUCTION

1.1 Introduction

All the governments in the world are enacting data protection laws that restrict the disclosure and handling a personal data. These laws enforce administrative and financial burdens on organizations that manage personal data and may constrain the permitted and valuable sharing and analysis of this data (Johnson and Grandison, 2007). A personal data is an information which relate to a person who can be identified from those data. These information is an important resource and asset to any organization.

Companies that gather and manage huge capacity of personal data are required by the principle of accountable data governance to take action to secure data subjects from any risks that might emerge from inappropriate uses of this data (Blocki *et al.*, 2012). Therefore, many organizations that using personal data in areas such as in Health Information System (HIS) has increasing their concerns in the right protection of these data.

A HIS is an integrated and comprehensive information system designed to handle the financial, clinical and administrative aspects of a hospital (Ismail *et al.*, 2010). The aim of HIS as a medical informatics area is to attain the most potential resources of administration and patient care by electronic data processing. One of the possible solution is to ensure the protection of information of the patient by information systems audit.

Information systems audit is defined as the well-ordered procedure of collecting, categorizing and assessing the evidence to decide whether an information system secures the assets, preserves the integrity of data, fulfils the aims of the organizations efficiently and utilizes supports effectively (Martínez *et al.*, 2010). Software audit, which is a special type of audit within this field, with purpose to justify the competence of both functional and non-functional requirements.

A medical data especially should be protected, and must be ensure on its data disclosure constraint. It should be ensure that medical information can only be used in a legalised medical environment. A proper system must be complied when transmitting information across context fields, for example, a consent should be receive for medical data to be disclose and should remain anonymous before it can be used in research medium (Pasquier and Eyers, 2016).

The Health Insurance Portability and Accountability Act (HIPAA) compromise a list of privacy requirements for protecting confidentiality and ensuring integrity of the personal data by ensuring the data only available to an authorize person only. However, to ensure the privacy requirements listed are followed, a data protection audit should be done. HIPAA has been followed by many countries, however, Malaysia does not following HIPAA. Yet, Malaysia has its own laws, regulations and also guidelines about the confidentiality and protection of personal data.

A data protection audit functions as a control tools and may determine the system weaknesses or prominence regarding the organization's managing the personal data. It is essential to determine security control for these sensitive data and its strategies to audit.

1.2 Problem Background

A personal data matter has become very important mostly in the healthcare system. The practice of medicine has been described as being overwhelmed by how well data is gathered, handled, recovered and conveyed. It is crucial to maintain the great working conditions for health experts to get to clinical information while HIS are still being evolved. The preservation of a patient confidentiality is of greatest importance in the doctor patient relationship.

The increased accessibility of health data in an electronic tools is good for industry-wide endeavour to enhance the standard and lessen the cost of healthcare, yet it leads to a related concern of large risk of privacy loss among health care participants. The medical services institutions are utilizing systems of electronic health record and patient portals to allow patients, staffs, and business associates more effective access to personal health data, however, there is a fear that the patients' privacy may not be capably protected if data managing systems are not cautiously planned and implemented (Datta *et al.*, 2011).

The US National Science Foundation-dependent Computing Research Association (CRA) has defined that the security of information systems and the protection of the end-users establish one of the significant global security-related problems (Smith and Spafford, 2004). However, regardless of existing laws regulating this aspect, a severe threat to privacy constantly take place. It is quite worrying as the patients are concern about the possibility of loss their personal information. This problem may become a serious matter if there is no solution to confront this problem.

1.3 Problem Statement

The increased availability of health data in an electronic tools is good for industry-wide efforts to enhance the quality and lessen the cost of healthcare. However, it brings a bigger concern of greater risk for loss of privacy among medical care participant. If the loss of privacy happens, it can weakens the quality of personal data especially on the patient records.

There are many algorithms and methods can be used for an assessment of personal data security. Each of the methods has their own advantages and disadvantages. Not all method are strong enough to use for a personal data security assessment.

Although various companies have described measures and controls which to do an assessment on information systems security, relatively few structured method that utilizes engineering method to handle an assessment process of information security which is as sensitive as data with ensures.

1.4 Project Research Aim

The aim of the project is to identify current practices of assessment on personal data security and propose a requirements engineering method on assessment of personal data security in public hospital in Malaysia.

1.5 Objectives

The objectives of this project are:

1) To identify practices or guidelines on personal data security related to the patient data.

2) To implement requirements engineering method on personal data security for healthcare.

3) To measure the requirements engineering method for personal data security in Klang hospital by conducting a survey and validation.

1.6 Research Scope

In order to achieve the objectives, the following scopes are outlined:

1) This project is focused on personal data security of patients in the public hospital. The effort highlight on providing a methods of assessment on personal data security related to the patient data.

2) The project used a requirements engineering method to assess the personal data security. It includes to protect the confidentiality and the privacy of personal data.

3) The requirements engineering process is validated through a data collection in Klang hospital. The data collection is through a questionnaire in order to get the feedback and response based on the requirements.

1.7 Research Contribution

From this project, one of the expected research contribution is that the methods and techniques related to project are analysed and the current practice of assessment on personal data security are identified. Besides, an assessment on personal data security can be adapted through a requirement engineering from this project.

Other than that, the expected contribution from this project is that the personal data audit method of this project can be applied to the public hospital in Malaysia.

1.8 Report Organization

This report consists of 5 chapters:

1) Chapter 1: Introduction to the research including background of project with purposes, aims and objectives, and identified problem related to it, scope of project and expected research contribution.

2) Chapter 2: Contains the overview of the area of research, previous and existing trends of research.

3) Chapter 3: Explanation of research methodology including the research framework, project plan and project deliverables.

4) Chapter 4: Design and Implementation of the project with the research requirements that will be used.

5) Chapter 5: Analysis and evaluation of the results and findings based on selected approach.

6) Chapter 6: Conclusion of the project based on the objectives and problems statement.

REFERENCES

Abdullah, M. *et al.* (2016) *Clinical Audit Handbook.*

Abdullah, Z. S. (2012) 'Hospital information systems implementation: Testing a structural model', *Information Science and Digital Content Technology (ICIDT), 2012 8th International Conference on*, 1, pp. 74–81.

Baloyi, N. and Kotzé, P. (2017a) 'Are Organisations in South Africa Ready to Comply with Personal Data Protection or Privacy Legislation and Regulations?', *IST-Africa Conference Proceedings*, pp. 1–11.

Baloyi, N. and Kotzé, P. (2017b) 'Do Users Know or Care About What is Done with their Personal Data : A South African Study', pp. 1–11.

Barca, C. C. *et al.* (2014) 'YourEHRM: Standard-based management of your personal healthcare information', *2014 IEEE-EMBS International Conference on Biomedical and Health Informatics, BHI 2014*, pp. 89–92. doi: 10.1109/BHI.2014.6864311.

Blocki, J. *et al.* (2012) 'Audit Mechanisms for Provable Risk Management and Accountable Data Governance'.

Datta, A. *et al.* (2011) 'Understanding and Protecting Privacy: Formal Semantics and Principled Audit Mechanisms', in Jajodia, S. and Mazumdar, C. (eds) *7th International Conference, ICISS*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–27. doi: 10.1007/978-3-642-25560-1_1.

Dong, X. *et al.* (2016) 'DSPM: A Platform for Personal Data Share and Privacy Protect Based on Metadata', *2016 13th International Conference on Embedded Software and Systems (ICESS)*, (Cm), pp. 182–185. doi: 10.1109/ICESS.2016.10.

Emeka, B. O. and Liu, S. (2017) 'Security requirement engineering using structured object-oriented formal language for m-banking applications', *Proceedings - 2017 IEEE International Conference on Software Quality, Reliability and Security, QRS 2017*, pp. 176–183. doi: 10.1109/QRS.2017.28.

Fischer, P. E. (2013) 'Data Protection Audit: The German Experience', *Springer-Verlag Berlin Heidelberg*, pp. 233–259. doi: 10.1145/2505515.2514691.

Han, Z., Sun, Y. and Wang, Y. (2013) 'Audit Recommendation for Privacy Protection in Personal Health Record Systems', pp. 533–538.

Hasan, R. *et al.* (2016) 'How Secure is the Healthcare Network from Insider Attacks ? An Audit Guideline for Vulnerability Analysis'. doi: 10.1109/COMPSAC.2016.129.

Ismail, A. *et al.* (2010) 'The implementation of Hospital Information System (HIS) in tertiary hospitals in Malaysia: a qualitative study', *Malaysian Journal of Public Health Medicine 2010*, 10(2), pp. 16–24.

Johnson, C. M. and Grandison, T. W. A. (2007) 'Compliance with data protection laws using Hippocratic Database active enforcement and auditing', *IBM Systems Journal*, 46(2), pp. 255–264. doi: 10.1147/sj.462.0255.

Kasuya, S. *et al.* (2017) 'Cyber-Enabled Well-Being Oriented Daily Living Support Based on Personal Data Analytics', *IEEE Transactions on Emerging Topics in Computing*, 6750(c). doi: 10.1109/TETC.2017.2763966.

Laws of Malaysia (2010) *Personal Data Protection Act 2010*, *Percetakan Nasional Malaysia Berhad*.

Makri, E.-L. and Lambrinoudakis, C. (2015) 'Privacy Principles: Towards a Common Privacy Audit Methodology', *Springer International Publishing Switzerland 2015*, 9264, pp. 219–234. doi: 10.1007/978-3-319-22906-5.

Martínez, M. A. *et al.* (2010) 'A Personal Data Audit Method through Requirements Engineering', *Computer Standards and Interfaces*. Elsevier B.V., 32(4), pp. 166–178. doi: 10.1016/j.csi.2010.01.001.

Mead, N. R., Shoemaker, D. and Ingalsbe, J. (2010) 'Teaching Security Requirements Engineering Using SQUARE'.

Milton Lum, S. W. *et al.* (2011) *Confidentiality Guidelines*. Available at: http://mmc.gov.my/v1/docs/2011 3 Confidentiality guidelines Approved on 11 October 2011_1.pdf.

Muyanja, A. *et al.* (2013) 'Requirements engineering for the uganda police force crime records management system', *2013 21st IEEE International Requirements Engineering Conference, RE 2013 - Proceedings*, pp. 302–307. doi: 10.1109/RE.2013.6636734.

Namoglu, N. and Ülgen, Y. (2014) 'Network Security Vulnerabilities and Personal Privacy Issues in Healthcare Information Systems : A Case Study in a Private Hospital', pp. 3–5.

Ouhbi, S. *et al.* (2017) 'E-health internationalization requirements for audit purposes', *Computer Methods and Programs in Biomedicine*. Elsevier Ireland Ltd, 144, pp. 49–60. doi: 10.1016/j.cmpb.2017.03.014.

Pasquier, T. F. J. M. and Eyers, D. (2016) 'Information flow audit for transparency and compliance in the handling of personal data', *Proceedings - 2016 IEEE International Conference on Cloud Engineering Workshops, IC2EW 2016*, pp. 112–117. doi: 10.1109/IC2EW.2016.29.

Patel, S. S. and Sankpal, S. V. (2016) 'Secure patients data transmission using XOR ciphering encryption and ECG steganography', *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, pp. 1311–1315. doi: 10.1109/ICEEOT.2016.7754895.

Peng, F. and Jiang, X. (2011) 'A Novel Education System Requirements Engineering Methodology', *IEEE 2011*, pp. 428–230.

Ratnam, K. A. and Dominic, P. D. D. (2011) 'A study of technology sustainability on hospital information management system (HIMS) Governance in Malaysia', *2011 National Postgraduate Conference - Energy and Sustainability: Exploring the Innovative Minds, NPC 2011*. doi: 10.1109/NatPC.2011.6136309.

Security Policy (2017). Available at: http://htar.moh.gov.my/en/polisi-keselamatan (Accessed: 15 August 2018).

Seong, K. (2009) *Defense Health Information System as a Case Study for National Health IT, Biomedical Informatics Session*.

Smith, S. W. and Spafford, E. H. (2004) 'Grand challenges in information security: process and output', *IEEE Security & Privacy*, 2(1), pp. 69–71. doi: 10.1109/MSECP.2004.1264859.

Will, M. A. *et al.* (2017) 'Returning control of data to users with a personal information crunch - A position paper', *Proceedings - 5th International Conference on Cloud Computing Research and Innovation, ICCCRI 2017*, pp. 23–32. doi: 10.1109/ICCCRI.2017.12.

Zailani, S. and Zalazilah, H. (2006) 'The Relationships Between the Extent of Information Systems Adoption and Service Performance in the Public Hospital in Malaysia', *2006 2nd International Conference on Information & Communication Technologies*, 1, pp. 471–472. doi: 10.1109/ICTTA.2006.1684415.