

Electronic Healthcare Information Security

Advances in Information Security

Sushil Jajodia

Consulting Editor

Center for Secure Information Systems

George Mason University

Fairfax, VA 22030-4444

email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Charles A. Shoniregun • Kudakwashe Dube
Fredrick Mtenzi

Electronic Healthcare Information Security

 Springer

Professor Charles A. Shoniregun
Infonomics Society
United Kingdom and Ireland
cshoniregun@infonomics-society.org

Dr. Kudakwashe Dube
Massey University
Computer Science and Information
Technology
School of Engineering & Advanced
Technology (SEAT)
Palmerston North 4442, New Zealand
K_Dube@massey.ac.nz

Dr. Fredrick Mtenzi
Dublin Institute of Technology
Kevin Street
Dublin 8
Ireland
fredr_mtenzi@comp.dit.ie

ISSN 1568-2633
ISBN 978-0-387-84817-4 e-ISBN 978-0-387-84919-5
DOI 10.1007/978-0-387-84919-5
Springer New York Dordrecht Heidelberg London

© Springer Science+Business Media, LLC 2010

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Dedications

To our families and friends ...

Acknowledgements

It is difficult to acknowledge all the people that have directly or indirectly contributed to this book. But some names cannot be forgotten many thanks to our editors Jennifer Maurer and Susan Lagerstrom-Fife.

A special thank you to the following people and families: Galyna Akmayeva, Tinashe Zakaria, Dr. Bing Wu, Professor Jane Grimson, Professor Brendan O'Shea, Mariam Mussa, Professor Hans Guesgen, Professor Elizabeth Kemp, The Shoniregun's family, The Dube's family, and The Mtenzi's family, for their never-ending contributions.

We are also deeply indebted to the security and privacy research community and our sincere thanks to all the organizations that voluntarily participated in our search for knowledge.

Preface

The adoption of Information and Communication Technologies (ICT) in healthcare is driven by the need to contain costs while maximizing quality and efficiency. However, ICT adoption for healthcare information management has brought far-reaching effects and implications on the spirit of the Hippocratic Oath, patient privacy and confidentiality. A wave of security breaches have led to pressing calls for opt-in and opt-out provisions where patients are free to choose to or not have their healthcare information collected and recorded within healthcare information systems. Such provisions have negative impact on cost, efficiency and quality of patient care. Thus determined efforts to gain patient trust is increasingly under consideration

for enforcement through legislation, standards, national policy frameworks and implementation systems geared towards closing gaps in ICT security frameworks.

The ever-increasing healthcare expenditure and pressing demand for improved quality and efficiency in patient care services are driving innovation in healthcare information management. Key among the main innovations is the introduction of new healthcare practice concepts such as shared care, evidence-based medicine, clinical practice guidelines and protocols, the cradle-to-grave health record and clinical workflow or careflow. Central to these organizational re-engineering innovations is the widespread adoption of Information and Communication Technologies (ICT) at national and regional levels, which has ushered in computer-based healthcare information management that is centred on the electronic healthcare record (EHR). A critical and determinant factor in this scenario is the heightened awareness and concern about ensuring patient privacy and confidentiality, which are under threat within the distributed networked environment of ICTs and EHRs. The domain of healthcare information management offers a significant, complex and challenging testing ground to Information Security due to the complex nature of healthcare information. The security of healthcare information in the context of a networked, sensor-enabled, pervasive and mobile computing infrastructure is at the core of both the main challenges and potential risks of Healthcare ICT adoption.

The domain of healthcare has become a challenging testing ground for information security due to the complex nature of healthcare information and individual privacy. This is the first comprehensive book that explores the challenges of Electronic Healthcare Information Security, Policies and Legislation. We proposed a framework and an evaluation approach for the e-Healthcare Information Systems Security. This book also reflects our knowledge and experience in the field of security and privacy.

London – UK, New Zealand and Dublin - Ireland
May 2010

Charles Shoniregun
Kudakwashe Dube
Fredrick Mtenzi

Contents

1	Introduction to e-Healthcare Information Security	1
1.1	Introduction	1
1.2	The e-Healthcare Information: Nature and Trends	1
1.3	Security Impact of Trends in e-Healthcare Information Management	3
1.4	Trends in e-Healthcare Environment	4
1.4.1	Case Study: Canada	5
1.4.2	Case Study: IZIP and General Health Insurance Company of the Czech Republic	8
1.4.3	Case Study: Danish Health Data Network (DHDN)	9
1.4.4	Case Study: The Norwegian Healthcare System	13
1.4.5	Case Study: Sweden	15
1.4.6	Case Study: UK - NHS Direct Online (NHSDO) Information Service	17
1.5	Securing e-Healthcare Information: Significance and Challenges ...	19
1.6	Concepts of e-Healthcare Information Security	20
1.7	Frameworks and Approaches	21
1.8	Issues in e-Healthcare Information Security	23
1.9	Summary	25
	References	25
2	Securing e-Healthcare Information	29
2.1	Introduction	29
2.2	Breaches of Privacy and Confidentiality in e-Healthcare	30
2.2.1	Accidental Privacy and Confidentiality Breaches	30
2.2.2	Ethically Questionable Conduct	31
2.2.3	Breaches Due to Illegal Actions	32
2.2.4	Laxity in Security for Sensitive e-Healthcare Information ...	32
2.3	The IT Security Challenge for Securing e-Healthcare Information ..	32
2.4	The Privacy and Confidentiality Challenge	33
2.5	Utilisation Challenges	35
2.6	Legal Protection Challenges	36

- 2.7 The Nature of Secure e-Healthcare Information 36
- 2.8 The Principles for Securing e-Healthcare Information 38
- 2.9 Combining Security with Privacy and Confidentiality 40
- 2.10 Identifiability in Securing e-Healthcare Information 42
- 2.11 Anonymisation and Pseudonymisation 43
- 2.12 Technological Frameworks in Securing e-Healthcare Information . . 45
- 2.13 Engineering of Secure e-Healthcare Information 47
 - 2.13.1 Methodologies for Engineering Secure e-Healthcare Information Systems 47
 - 2.13.2 Measures and Security Metrics for Securing e-Healthcare Information 49
 - 2.13.3 Evaluation of Secure e-Healthcare Information 50
- 2.14 Discussion and Summary of Issues in Securing e-Healthcare Information 50
- References 51

- 3 Laws and Standards for Secure e-Healthcare Information 59**
 - 3.1 Introduction 59
 - 3.2 The Rationale for Laws and Standards in Securing e-Healthcare Information 60
 - 3.3 Laws and Standards: Relationships, Roles and Interactions 61
 - 3.4 Legal Protection of Privacy in e-Healthcare Information Management 62
 - 3.4.1 International and EU Law on Protection of e-Healthcare Information 62
 - 3.4.2 Irish Law on Protection of e-Healthcare Information 64
 - 3.4.3 UK Law on Protection of e-Healthcare Information 66
 - 3.4.4 Australian Law on Protection of e-Healthcare Information . . 66
 - 3.4.5 New Zealand Law on Protection of e-Healthcare Information 66
 - 3.4.6 Japanese Law on Protection of e-Healthcare Information . . 67
 - 3.4.7 US Law on Protection of e-Healthcare Information 67
 - 3.4.8 Canadian Law on Protection of e-Healthcare Information . . 71
 - 3.5 Standards for Secure e-Healthcare Information 72
 - 3.5.1 Health Level 7 (HL7) Standardisation 72
 - 3.5.2 Committee for European Normalisation (CEN) Technical Committee (TC) 251 Standardisation 74
 - 3.5.3 The openEHR Specification Standard 75
 - 3.5.4 International Standards Organisation Technical Committee (ISO/TC) 215 Healthcare Informatics Standardisation 78
 - 3.5.5 ASTM Committee E31 on Healthcare Informatics Standardisation 79
 - 3.5.6 Generic IT Security within e-Healthcare Information Management 84
 - 3.6 Discussion and Summary of the Legal and Standardisation Challenges 93

- 3.7 Summary 95
- References 96

- 4 Secure e-Healthcare Information Systems 101**
 - 4.1 Introduction 101
 - 4.2 The elements of Security and Privacy in e-Healthcare Information Systems 102
 - 4.3 Security and Privacy Provisions in EHR Systems 104
 - 4.3.1 The Canadian Health Infoway 105
 - 4.3.2 Security and Privacy Provisions in the UK NHS Care Records 106
 - 4.3.3 Security and Privacy Provisions in the WorldVistA EHR System 108
 - 4.4 Security and Privacy Provisions in Electronic Personal Healthcare Records 109
 - 4.4.1 Google Health e-PHR 110
 - 4.4.2 The Microsoft e-PHR service: The HealthVault 111
 - 4.4.3 The Indivo Open Source e-PHR system 112
 - 4.4.4 Summary of Concerns and Issues with e-PHR systems and Services 112
 - 4.5 Security and Privacy in Clinical Decision Support Systems 114
 - 4.6 The Challenges from Security and Privacy for e-Healthcare Information Security 117
 - 4.7 Future e-Healthcare Information Management: Towards the EHR/PEHR Hybridisation 118
 - 4.8 Summary 120
 - References 121

- 5 Towards a Comprehensive Framework for Secure e-Healthcare Information 123**
 - 5.1 Introduction 123
 - 5.2 The Problem of Securing e-Healthcare Information 124
 - 5.3 The Context and Concepts for Securing e-Healthcare Information .. 125
 - 5.4 Towards Future-Enabled Requirements for Securing e-Healthcare Information 128
 - 5.4.1 The Security and Privacy Impact of the Evolution of the Control of e-Healthcare Information in Context of the Patient-Centred Paradigm 129
 - 5.4.2 The nature, security and privacy implications of the EHR/PEHR hybrid 132
 - 5.4.3 The Role of Security Metrics 134
 - 5.4.4 Summary of Security and Privacy Requirements for Future-Enabled e-Healthcare Information 135
 - 5.5 The Approach to Securing e-Healthcare Information 135

- 5.6 The Framework for Securing e-Healthcare Information Security and Privacy 137
 - 5.6.1 The Key Drivers to the Security and Privacy of e-Healthcare Information Security 138
 - 5.6.2 The Model for the e-Healthcare Information Control and Security and Privacy Risk Level Over Time 140
 - 5.6.3 The Conceptual Framework for Secure e-Health Information 144
- 5.7 The Conceptual Architecture 146
- 5.8 Discussion and Summary 148
- References 150

- 6 Towards a Unified Security Evaluation Framework for e-Healthcare Information Systems 151**
 - 6.1 Introduction 151
 - 6.2 Evaluating Privacy and Security in e-Healthcare 151
 - 6.3 Approaches to Evaluation of e-Healthcare Information Security and Privacy 153
 - 6.3.1 Standards-Based Security and Privacy Evaluation 153
 - 6.3.2 Privacy Policy Evaluation 153
 - 6.3.3 Ontology-Based Privacy Evaluation 154
 - 6.3.4 Security and Privacy Metrics 154
 - 6.3.5 Model-Based Approach to Security and Privacy Evaluation 160
 - 6.4 Frameworks for e-Healthcare Information Privacy and Security Evaluation 160
 - 6.4.1 Information Security Management Model-Based Evaluation Frameworks 160
 - 6.4.2 Security Metric-Based Evaluation Frameworks 161
 - 6.4.3 Security and Privacy Policy-Based Evaluation Frameworks 161
 - 6.5 Towards a Unified Privacy and Security Evaluation Framework for e-Healthcare Information 162
 - 6.5.1 The Security and Privacy Evaluation Challenges for e-Healthcare Information 162
 - 6.5.2 Towards a Unified Framework for Evaluating Privacy and Security of e-Healthcare Information 163
 - 6.6 Human Factors in Evaluating e-Healthcare Information Security and Privacy 167
 - 6.6.1 Impact of Technological Human Factors 167
 - 6.7 Summary 168
 - References 169

- 7 Discussions 173**
 - 7.1 Introduction 173
 - 7.2 Securing Personal e-Healthcare 174
 - 7.3 Proliferation of New Technologies 176
 - 7.4 Health Identifier 178

7.5 Problem of Securing e-Healthcare Information 179
7.6 Contribution to Knowledge 181
7.7 Conclusion 182
7.8 Future Work and Research Directions 182
References 183

**A International Standards Organisational Technical Committee
(ISO/TC) 215 Healthcare Informatics Standardisation 185**

List of Figures

1.1	The Healthcare Process Supported by the DHDN	11
1.2	No Direct Connection between Individual Pharmacies and the NIA ..	14
1.3	The Role of NHSDO	18
1.4	Major issues in e-Healthcare security	24
2.1	Major issues in Securing e-Healthcare Information	30
3.1	Major issues in Laws and Standards for Secure e-Healthcare Information	60
4.1	Current and future e-Healthcare Information Systems	102
4.2	The evolution of e-healthcare information systems	103
4.3	Security Issues in CPG Management	116
4.4	The move towards hybrid e-Healthcare information systems and away from pure EHR and PEHR systems	119
5.1	The Contextual Framework for e-Healthcare Information Security and Privacy	126
5.2	The Evolution of e-Healthcare Information Management and Future of EHR/PEHR	130
5.3	Characteristics of the PEHR/EHR Hybrid	133
5.4	The Pyramid of Security and Privacy for e-Healthcare Information ..	137
5.5	The drivers to e-Healthcare information security and privacy	138
5.6	The Graph of “e-Healthcare Information control” or “Security and Privacy Risk Level” over time	140
5.7	Security and Privacy Characterisation Framework	144
5.8	The process of establishing a secure e-Healthcare information infrastructure	146
5.9	The e-Healthcare Information Privacy and Security Conceptual Architecture	148

- 6.1 The ACIO Framework for the evaluation of security and privacy for e-Healthcare Information 165
- 6.2 The spinning discs illustrating the dynamics of the ACIO framework 166

List of Tables

3.1	Published CEN TR XXXXX Standards of CEN/TC 251	74
3.2	Published CEN TS XXXXX standards of CEN/TC 251	75
3.3	Published CR XXXXX Standards of CEN/TC 251	75
3.4	Published EN XXXXX standards of CEN/TC 251	76
3.5	Published ISO-Related Standards of CEN/TC 251	77
3.6	Published ENV XXXX standards of CEN/TC 251	77
3.7	ASTM Committee E31 Standards for Security and Privacy in Healthcare Informatics	79
3.8	ASTM Committee E31 Standards for Healthcare Vocabularies	80
3.9	ASTM Committee E31 Standards for Documentation in Healthcare ..	80
3.10	ASTM Committee E31 Standards for Modelling and E-Healthcare Records	80
4.1	Elements of Privacy and Security in e-HIS based on ISO/TS 18308 ..	104
4.2	Services within the Canadian Health Infoway Privacy and Security Conceptual Architecture (PSCA)	107
4.3	Comparison of e-PHR systems	114
4.4	Summary of Security Challenges facing modern e-HIS	117
5.1	Characteristics of the EHR/PEHR Hybrid	134
A.1	Security and Privacy Standards of the ISO/TC 215 - Health informatics	185
A.2	ISO/IEEE Standards of the TC 215 - Health informatics	186
A.3	ISO Standards of the TC 215 - Health informatics	186
A.4	ISO/TS Standards of the TC 215 - Health informatics	187
A.5	ISO/TR Standards of the TC 215 - Health informatics	187

LIST OF CONTRIBUTORS AND ORGANISATIONS

Deloitte LLP, United Kingdom

Environmental Policy Research Centre, Germany

Empirica Gesellschaft fuer Kommunikations und Technologieforschung mbH, Germany

ESYS Consultancy, United Kingdom

IBM, USA

Information and Communications Technology Council, Canada

Infonomics Society, United Kingdom and Ireland

Dublin Institute of technology, Ireland

InternetSecurity.com

Jagiellonian University, Poland

KADRIS Consultants, France

Massey University, Palmerston North and Auckland, New Zealand

Microsoft Corp, USA

TanJent Consultancy, United Kingdom

University of KwaZulu-Natal, South Africa

University of Potsdam, Sweden

University of Zimbabwe, Harare, Zimbabwe

National University of Science and Technology, Bulawayo, Zimbabwe

University of Dar es Salaam, Dar es Salaam, Tanzania

Data Management Solutions Technologies Limited, Dar es Salaam, Tanzania