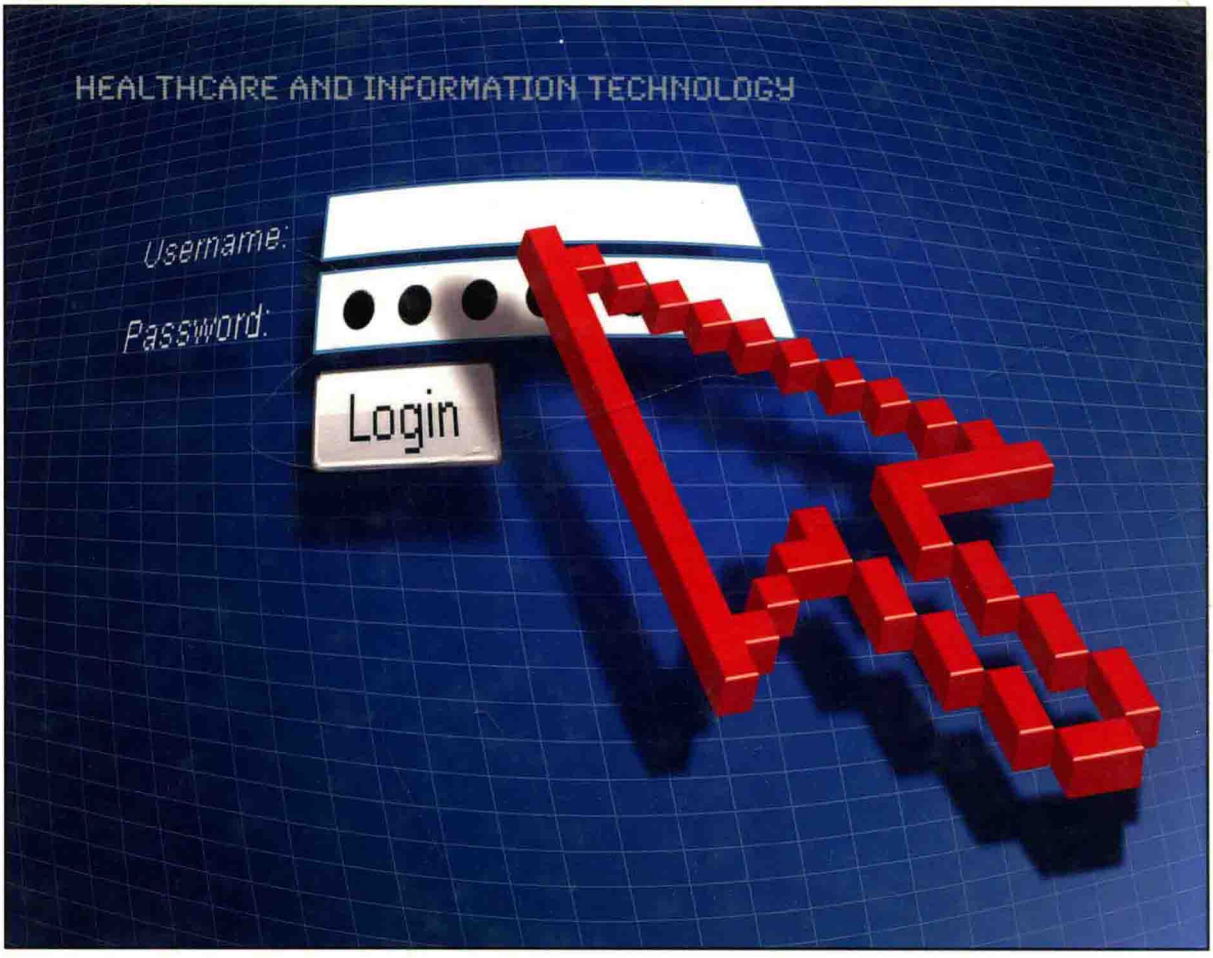
PREMIER REFERENCE SOURCE

Certification and Security in Health-Related Web Applications

Concepts and Solutions



Anargyros Chryssanthou, Ioannis Apostolakis & Iraklis Varlamis

Certification and Security in Health-Related Web Applications:

Concepts and Solutions

Anargyros Chryssanthou
Hellenic Data Protection Authority, Greece

Ioannis Apostolakis
National School of Public Health, Greece

Iraklis Varlamis
Harokopio University of Athens, Greece

Medical Information Science REFERENCE

MEDICAL INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Dave DeRicco
Publishing Assistant: Milan Vracarich Jr.
Typesetter: Michael Brehm
Production Editor: Jamie Snavely
Cover Design: Lisa Tosheff

Published in the United States of America by
Medical Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Certification and security in health-related web applications : concepts and solutions / Anargyros Chryssanthou, Ioannis Apostolakis and Iraklis Varlamis, editors.
p. cm.
Includes bibliographical references and index.
Summary: "This book aims to bridge the worlds of healthcare and information technology, increase the security awareness of professionals, students and users and highlight the recent advances in certification and security in health-related Web applications"--Provided by publisher.
ISBN 978-1-61692-895-7 (hardcover) -- ISBN 978-1-61692-897-1 (ebook) 1. Medical informatics--Security measures. 2. Medicine--Databases--Security measures. 3. Medicine--Databases--Certification. 4. Internet in medicine--Security measures. I. Chryssanthou, Anargyros, 1979- II. Apostolakis, Ioannis, 1961- III. Varlamis, Iraklis, 1974-
R859.7.S43C47 2011
610.285--dc22
2010016324

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Editorial Advisory Board

List of Reviewers

Foreword

Over the last few years, the immense need to develop and organize new ways for providing accessible, responsive, timely, effective, safe, qualitative and efficient health care, has fortunately been accompanied by significant advances in the field of information and communication technology. The application of these advances in most areas of health care delivery had truly dramatic and revolutionary effects. In fact there are major progresses in the health care sector over the past years, but the realm of health information technology is unique.

Specifically, health care information and communication technology is indispensable for overcoming fragmented systems and services and for achieving cost savings, as well as productivity and efficiency gains in the organization and funding of health care. In addition, it ensures the timely and accurate collection, exchange and availability of data, which are critical for the provision of safe, qualitative and effective care. Furthermore, it facilitates online access to clinical guidelines and drug databases, provides health care practitioners with evidence-based clinical information at the point of care and facilitates their interaction with patients and other stakeholders. On the other hand, it also gives patients the ability to obtain information to better manage their condition and to communicate with the health system, a fact that could also improve the efficiency and quality of care.

Technology has recently made it possible to exchange health data over the internet or thought web and wireless systems and applications, a technical evolution which raises significant challenges with regards to the credibility, accountability, safety, confidentiality, integrity, availability and privacy of services, information and resources. In this light, a main challenge relates to the fact that the sector struggles with inconsistent medical terminology, clinical records and data storage, as well as a multiplicity of schemes introduced to facilitate interconnection and communication between specific information systems. This fragmentation and the rapidly evolving nature of technological solutions, in the absence of agreed industry-wide standards, expose providers investing in technological infrastructure to high risks of failure and poor returns. The interoperability of the systems is dependent upon adopting common standards and achieving compliance with them.

Moreover, another significant challenge relates to enabling robust and reliable privacy and security frameworks. Specifically, because of the sensitivity of health information and the generalized uncertainty on how existing legal frameworks apply to health information technology systems, privacy concerns constitute one of the most difficult barriers in the wider implementation of information technology. Health information can be extremely sensitive, while professional ethics in health care demands a strict adherence to strict confidentiality and legal rules. Hence, there appears to be a generalized need for clear and enforceable systems and rules on these sensitive issues.

In light of the above mentioned, the present book represents a significant contribution in the field, which provides relevant and newest theoretical frameworks and references to the most recent empirical research findings in this area. In particular, it deals with the issue of access control and secure exchange of health information over the internet through web healthcare and related information systems. It attempts to deal with issues relating to certification and security procedures, to identify open threats and emerging needs and to provide solutions to the various challenges. Indeed, it constitutes a valuable tool for every professional intending to develop or support a health related application over the internet or participate in such an application. As such a tool, this book will increase the interaction between health care, health administration and health information technology professionals and all other interested parties.

Nikos Maniadakis
National School of Public Health, Greece

Nikos Maniadakis *is Chair at the Department of Health Services Management at the National School of Public Health in Greece and Director of the corresponding MSc programme. He holds a BSc in Economics from the University of Athens, an MSc in Health Economics from the University of York and a PhD in Business Studies from Warwick Business School. He was Research Fellow at Oxford and Warwick University and Senior Manager at the pharmaceutical companies Pharmacia and Eli Lilly. He also served as a CEO and President of the University Hospitals of Patras and Heraklion in Greece. He has been advisor to many private, governmental and European organisations and is member of several professional societies and referee to prominent journals in health services research. He is co-author to several articles in peer reviewed journals, has presented to a number of international conferences and lectures health care management in several international schools.*

Foreword

The healthcare sector is an indicative example of an application area that can benefit a lot from the development of a Web-based infrastructure. E-health networks enable integrated healthcare services in the form of electronic health records accessible via Internet technology. During the last years, with the adoption of Electronic Health Records, a steadily increasing number of health-related Web applications have been made available to providers, practitioners, researchers and patients. While this development offers important benefits, there are security and privacy concerns integral to the process of electronic healthcare delivery. Ensuring secure access to Electronic Healthcare Records and protecting the privacy of patient information are two issues of paramount importance when it comes to the design of health related web applications. Efficiency and effectiveness of information security policy is crucial, especially when dealing with applications that may affect patients' rights and interests. One of the biggest challenges in implementing e-health concepts is convincing the individuals sharing their electronic health records that their data will be safe and secure. This book discusses theoretical issues as well as empirical findings and case studies in health related web applications. Divided into seven parts including fourteen chapters, this volume addresses the most aspects of this area.

The first section (chapters 1-2) deals with access control: The authors of Chapter 1 present an approach based on attribute-based encryption to protect the confidentiality of patients' information during the exchange of electronic health records among healthcare providers. In Chapter 2 the authors review possible threats and vulnerabilities and present a hierarchical access control model that, from a security policy perspective, refers to data ownership and access control issues.

Section 2 (chapters 3-5) refers to the goal of increasing the flexibility of access control mechanisms. In Chapter 3 a context-aware authorization model is presented, which ensures provision of tight, just-in-time access according to the current context. The main contribution of Chapter 4 consists in the proposed privacy protection architecture called PRIMA aiming at reconciling security and privacy policies with the actual healthcare workflow, while the purpose of Chapter 5 is to present an interplay of flexibility and multi-level security, perceived as important structural and behavioral features of robust intelligence in careflow systems.

The third section (chapters 6-7) deals with evaluation and certification of security measures. With focus on ISO/IEC 27000:2009, Chapter 6 offers an overview of information security management standards in the context of healthcare information systems and provides a guide to develop a complete and robust information security management system for healthcare organizations. Chapter 7 focuses on reliability features of Electronic Health Records and emphasizes the need to develop a Web security vulnerabilities framework reflecting the service deployment environment.

Section 4 (chapters 8-10) is about the issue of trust in healthcare networks and communities. Chapter 8 highlights the necessity to address issues around security, privacy and trust in a systematic manner

and tackle legal, business and technical issues that arise when providing electronic healthcare services. Chapter 9 deals with certification and security issues in biomedical grid portals and presents the security infrastructure of GRISSOM (Grids for In Silico Systems biology and Medicine) platform. Chapter 10 discusses the key debates with respect to Medicine 2.0 and Health 2.0 and possible privacy concerns about disintermediation between patients and health professionals and over reliance on virtual interactions.

The issue of security in wireless and mobile healthcare applications is dealt with in Section 5. Chapter 11 studies the issues of secure collection and transfer of physiological data from mobile or remote patients through a TETRA network.

Section 6 (chapter 12) deals with legal aspects of security. It discusses the issues of online advertising of health related products and services and stresses the risks for the privacy and safety of consumers, while presenting the EU legal framework.

The last section (Section 7 – chapters 13 and 14) refers to the perception of security by healthcare professionals. Password sharing is a common practice in the health sector which simultaneously constitutes a crucial security problem when providing electronic healthcare services. Chapter 13 suggests some solutions to the problem of password authentication using both technological and social cultural mechanisms. By empirically assessing the intention of and the attitude of nursing students in relation to security practices, Chapter 14 highlights the significant effects of perceived benefits, general security orientation and self-efficacy to behavioral intention of nursing students in applying security concepts and practices.

This volume deals with one of the most crucial issues in the area of e-health. Adopting a holistic approach this book attempts to close the gap between theory and praxis, between a pure technological approach and other aspects of security in web-based health related applications. The authors provide relevant theoretical frameworks and the latest empirical research findings. In this perspective this volume achieves its aim and increases interaction between members of the medical community, researchers, IT professionals and all other interested parties, such as patient organisations etc. The readers will be stimulated in their own research in the field of security in Electronic Health Records and the relevant web-based applications. It is also a highly educational text for anybody who wants to understand this area. Covering many security and certification issues and discussing case studies, this volume is a valuable reference book for security in web based health related applications.

Lilian Mitrou
University of the Aegean, Greece

Lilian Mitrou *is Assistant Professor at the University of the Aegean-Greece (Department of Information and Communication Systems Engineering) and Visiting Professor at the Athens University of Economics (Postgraduate Studies Program). She teaches information law and data protection law. She has served as a Member of the Hellenic Data Protection Authority (1999-2003) and as an Advisor to the former Prime Minister K. Simitis in sectors of Information Society and Public Administration (1996 - 2004). From 1998 till 2004 she was the national representative in the EC- Committee on the Protection of Individuals with regard to the Processing of Personal Data. She served as member of many Committees working on law proposals in the fields of privacy and data protection, communications law, e-government etc. Her professional experience includes senior consulting and researcher positions in a number of private and public institutions on national and international level. Her research interests include: Privacy and Data Protection; e-Democracy and eGovernment services; Internet Law. L. Mitrou published books and chapters in books (in Greek, German and English) and many journal and conference papers.*

Preface

CERTIFICATION AND SECURITY IN HEALTHCARE

Advances in telecommunications and informatics have provided humanity with the opportunity to provide advanced services to people world-wide. One of the areas that have most benefited from information technology is the health sector. Health-related web applications have provided advanced services, such as telemedicine, to patients and doctors. However, these applications have brought along several responsibilities: to record, process and store medical information by following standard and lawful procedures, to protect medical data from unauthorized access, to ensure continuity and constant availability of healthcare services, etc.

The Web attracted more patients in this way increasing the popularity of freely available medical advice and knowledge. The abundance of web sites that offer medical content affected the way patients face their doctors, gave them a second opinion and increased their awareness. Its' successor, Web 2.0, was built on the same technologies and concepts, but also added a layer of semantic abstraction, offered a network as a platform sensation and gave a social networking aspect to healthcare and medical applications.

The web offers access to many databases that contain medical information, and has significantly changed the way patients seek medical help. According to recent surveys, 50% of patients access medical information via the internet before visiting their doctor and this information affects their choice of treatment. The assistant role of virtual communities for patients who seek for medical help and advice is undeniable. Researchers, practitioners, medical industry and patients jointly contribute their findings, products and experiences, to the community's knowledge base. The information transferred inside a health related virtual community and the stockpiled knowledge must be carefully protected from unauthorized use and validated in order to be qualitative and useful.

With the use of web-based healthcare applications, such as telemedicine, tele-healthcare, tele-homecare etc, doctors are able to provide medical services to patients in distant and isolated areas. All these applications assume that medical data, such as vital signs and a patient's medical profile, are transferred securely and reliably over the complex infrastructure of the World Wide Web. Moreover, they assume the trustfulness of the source and destination of medical data.

Till now, the most widely used service is the distribution of informative content (i.e. medical documents, surveys, medical advices, news etc.). Content should be easily located and retrieved from patients. In order to facilitate new users, content can be forwarded to patients via appropriate services. However, information dissemination inside a medical community needs to be secured and certified. For example, dissemination via mailing lists requires security measures to be taken, in order to ensure the safe transfer

of medical data, while medical rss feeds require validation and certification concerning their sources. In the former case (website transmission) cryptographic protocols, such as SSL (Secure Socket Layer), can be used by a member to communicate with the community site, whereas in the latter case a respectful healthcare association is required to certify the feed sources.

In the case of telemedicine systems, for example, a patient's medical profile and other medical information are transferred over the network from the examination lab to the doctor's office in order for the doctor to be able to perform a diagnosis. According to the CIA model (confidentiality, integrity and availability), the medical information transferred across the network should be encrypted, secured and protected until it reaches its final destination. Patients' medical profiles should be accessible by their doctors in order to support diagnosis and care, but must be invisible to other patients, medical companies or individuals who don't have the appropriate privileges. Moreover, medical data should be preserved for future use and must always be available, although protected from unauthorized alterations. The use of standards in the whole process of collecting, transferring, storing and managing sensitive medical data is a requirement and should be accompanied by auxiliary auditing and monitoring services in order to build a trust model between patients and doctors.

Security in Health-Related Web Applications has many aspects such as: a) authentication, which guarantees that medical data and consultation are genuine, b) authorization, which assures that medical data are accessed by appropriate right holders, thus reinforcing trust between the partners of a medical transaction, c) non-repudiation, which guarantees that both trustees will fulfill their obligations to a contract and will acknowledge all conducted transactions, thus gradually enhancing the bonds between partners, d) risk management which refers to the ongoing iterative process of assessing web based applications for vulnerabilities, reinforcing them against threats and implementing appropriate security controls.

Certification is an addition to traditional aspects of security and is a means of guaranteeing that medical data are exchanged and processed appropriately. It requires auditing and ensures appropriateness of the medical process in terms of information security and compliance to suitable standards and regulations (ISO/IEC 27000 series, HIPAA directions and data protection laws).

Methodologically, taking security measures may maintain integrity, ensure availability and protect confidentiality however it does not guarantee the "ultimate" level of computer security. In the case of transferring medical data across complex computer networks, it might not suffice to secure the exchanging endpoints. Throughout its lifecycle, medical data is vulnerable to unauthorized access, alteration or manipulation, which without any security checks or presence of auditing procedures can easily go undetected, and weaken its reliability. In a secure lifecycle, medical data is managed and protected so that it remains authentic, reliable and useable, while retaining its integrity. These attributes of medical data can be preserved by implementing an effective Information Security Management System (ISMS) for Medical Information that ensures all three aspects of the aforementioned CIA model by implementing policies and procedures, allocating human and machine resources for all physical, personal and organizational aspects. Implementing an ISMS is not just putting measures in place, it means also auditing the system, evaluating its effectiveness and correcting it based on any identified security vulnerabilities or pitfalls, whether a security problem is caused from a human mistake or a manufacturer error.

Certification in web applications springs from the need to verify the accurate, impervious and protected exchange of data across the web. The persons accessing medical data, as well as the exchanging parties during transfers of medical data need to be accurately identified. Certifying these issues means that an auditing body can track down responsibilities and identify the culprit responsible for any breach of security, in any of the following areas: confidentiality, integrity, availability, authorization, non-repudiation.

These issues are of extreme importance when applied to medical virtual communities and the assistant role they provide to patients who seek for medical help and advice. In such communities it is important that the information transferred inside the community and the stockpiled knowledge is carefully protected from unauthorized access or use and validated in order to be qualitative and useful.

Summarizing all the above issues, any health-related web application (tele-medicine, tele-healthcare, tele-consultation etc.) must be examined under the prism of certification, security and confidentiality, but also fulfill authentication and non-repudiation requirements, thus providing a holistic approach in building trust within a networked web of medical information and tele-services. Developers of web based medical applications should also consider how certification applies in their applications. In the following section we depict the critical issues on building, maintaining, securing and certifying health related applications and summarize the available solutions.

SECURITY RISKS AND COMPLIANCE TO STANDARDS

As telemedicine applications evolve, the amount of sensitive information that travels through the World Wide Web increases and subsequently more strict security measures need to be taken in order to protect this information from unauthorized access. The measures can vary from simple password encryption policies to advanced cryptographic methods such as elliptic curves. For example a medical web community can employ Virtual Private Network technology as an access control measure for its users. A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Since the users of the health community connect to the application via an encrypted tunnel, any conducted communication is private and therefore secure. However, this is not always sufficient to build trust between the users of the community, thus certification is another step forward.

The ISO/IEC 27000 series of standards intends to cover all the different levels and aspects of security, such as auditing of the data transfer process, assessment of information security risks, implementation of information security controls and continuous monitoring, maintenance and improvement of information security. Data protection authorities can associate the level of provided protection with the applied security measures and certify whether an organization is providing adequate level of protection for medical data. It needs to be examined whether an authoritative party, such as a national health association, the world health organization or the EU, is providing specific guidelines for taking appropriate security measures for medical data and achieving an adequate level of protection.

An integral part of the ISO/IEC 27000 series in regards to health information systems, is the ISO/IEC 27799:2008 standard, which defines guidelines to support the interpretation and implementation of ISO/IEC 27002:2005 in health informatics. It specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. Healthcare organizations that comply with this standard ensure a minimum level of security and maintain confidentiality, integrity and availability of personal health information. Although the development of a security management system, which follows the ISO 27799:2008 directives, is a complicated task it is the first step in providing secure and trustful web based healthcare applications. Defining a clear and concise ISMS policy, which leads to the implementation of information security policies, is the real source pool for hardening the strength of a security management system. These policies can be systemic (e.g. access control policy), data (e.g. privacy policy) or human related (rules of conduct).

The Health Insurance Portability and Accountability Act of 1996 is an attempt to use federal law in order to protect the privacy of medical records. The implementation of the HIPAA privacy regulations proved to be costly, inconsistent, and frustrating to both physicians and patients. Moreover, healthcare applications on the web usually cross national borders and as such, they face several legal issues, such as licensing, accreditation, concerns of identity theft and dependency, which are difficult to be properly addressed by legislative entities.

The opt-out policy adopted by the U.S. Government defines that companies cannot collect consumer's data if the consumer asks for it. Concerning medical information, U.S. laws assume total confidentiality in several issues (i.e. abortions, contraception or psychological diseases) but delegate decisions to the state laws in others. European Union has adopted an opt-in model for all personal data, which assumes that all personal information is classified until their owner grants access on them. According to the EC directive for medical data protection (95/46/EC), only health professionals can access medical information and are responsible for protecting confidentiality. According to the Recommendation (97) 5, medical data can be collected without user consent, only for preventing a real danger or in the case of a criminal offence. Moreover, if the law provides for this, data may be collected and processed in order to preserve vital interests of the data subject, or of a third person. In the case of genetic data this includes the members of the data subject's genetic line.

TARGET AUDIENCE

Students of management of healthcare systems and healthcare managers in general will use this book as a companion that helps them avoid design pitfalls and provides a walkthrough towards building trustful healthcare applications. More specifically, managers will understand what is critical and what is not, always in terms of security, and will be facilitated when taking strategic decisions that concern the Health Information Systems.

Medical professionals will use the book as a reference, a gateway which can lead to potential solutions for issues, which just lurk in the background. More specifically, they will learn how to protect their patients and themselves, from loss or theft of information and they will better understand the needs of the medical community. Furthermore, they will be able to identify the need for a security oriented mentality which will prohibit them away from dwelling into security pitfalls with even legal consequences.

Members of the pharmaceutical profession will identify the value of security when using health web applications and learn the pitfalls that lurk in the World Wide Web when not being able to identify the requestor of medical information or the providing hand of pharmaceutical products by means of internet pharmacies.

Security professionals working in medical institutions will be able to identify the specific requirements of the medical community, learn how medical practitioners perceive security and thus implement the proper measures to achieve an adequate level of security for medical data.

Security auditors, who aim to audit healthcare organizations, can identify by reading this book the security problems of health information systems in general and health web applications in particular, in order to build a concrete methodology in their line of work in regards to medical applications.

Computer science and medical students will get informed on the new advances in security, certification and building of trust in a healthcare community.

This book aims to bridge the two worlds of healthcare and information technology, to increase the security awareness of professionals, students and users from both worlds and to highlight the recent advances in certification and security in health related web applications.

THE CHAPTERS

The book includes fourteen chapters that cover many different aspects of security and certification in health related web applications, ranging from the legal and ethical issues that concern the use and dissemination of medical data to different flexible data access control models and to the difficult task of increasing security awareness of users.

In the first chapter, entitled *Secure Exchange of Electronic Health Records*, the authors examine the traditional approaches in data access control, such as Mandatory Access Control, Discretionary Access control and Role-Based Access Control in terms of a shared care environment, where many medical professionals cooperate and exchange patient information. After a comparison of access control policies, the authors conclude that a shared care environment must define which information is collected, stored and accessed and suggest a flexible access control mechanism that protects privacy of patients and guarantees authorized access to stored data. The attribute-based encryption model allows the encryption of different sections of an electronic health record, which can be decrypted only by the owners of the proper key. Patients grant access to their doctors, who consequently are able to delegate access to collaborating physicians.

In the second chapter, entitled *Modeling Access Control in Healthcare Organizations*, the authors examine the security of hospital applications. They first explore issues in managing access control and security of healthcare information and review the possible threats and vulnerabilities for a hospital security plan, such as hardware or software failure, weak passwords and password stealing, misuse and abuse of the hospital information system etc. The paper introduces a hierarchical access model, which covers data ownership and access control issues and discusses the security issues that arise.

In chapter three, *A Context-Aware Authorization Model for Process-Oriented Personal Health Record Systems*, authors assume a process-oriented approach in Patient Health Records management and present a security framework that addresses several authorization and access control issues. The proposed framework capitalizes on tight and just-in-time authorization in order to guarantee that only authorized users get access to patient data and only for performing a specific task. A set of permissions, which is continuously adjusted in order to adapt to the changing context, reduces the risk of compromising information integrity during task execution.

The fourth chapter, entitled *Improving Security Policy Coverage in Healthcare*, presents a privacy protection architecture called PRIMA, which attempts to increase the usability of healthcare applications without compromising the security of patient information. The components of the PRIMA architecture guarantee policy definition, auditing of actions and restrictions throughout the clinical process and refinement of the original policies per case. As a result, the security policies and exceptions are more precise and realistic and fit to the clinical workflow instead of impeding it, thus enabling improved privacy protection for the patient and increased usability of the clinical workflow.

The fifth chapter, entitled *Flexibility and Security of Careflow Systems Modeled by Petri Nets*, deals with design and analysis of healthcare workflow systems and provides a solution that improves their structural and behavioral flexibility. Giving emphasis on flexibility, without neglecting security, secu-

rity in careflow systems is conceptually modeled using Petri nets and colored Petri nets. In this model, security and flexibility are covered separately and incrementally in sequential order. Dynamic change, case handling and mainly worklets are employed for increasing workflow flexibility in design and run time and consequently security models are applied in each step of the careflow system.

Chapter six, *Information Security Standards for Health Information Systems: The Implementer's Approach*, provides an overview of information security management standards in the context of health care information systems and focuses on the most widely accepted ISO/IEC 27000 family of standards for information security management. The chapter is a guide for developing a complete and robust information security management system for a health care organization, which mentions special implications that are met in a health care organization, as well as special considerations related to health related web applications. The guide is based on special requirements set by ISO/IEC 27799:2008.

Chapter seven, *Statistical Models for EHR Security in Web Healthcare Information Systems*, capitalizes on the quality and reliability issues of web information systems in healthcare. It presents how a wrong security policy decreases the reliability of the system and consequently deteriorates its overall quality and suggests several statistical models for evaluating the reliability of software. The modelling and study of the reliability of an EHR, especially when it is based on a service-oriented architecture, is performed with statistical models and measures called web metrics which assess the performance of health related applications and alert when reliability reaches critical levels.

Chapter eight, entitled *Identity Management and Audit Trail Support for Privacy Protection in E-Health Networks*, focuses in e-health networks and privacy protection. Since e-health networks can improve the efficiency and quality of care, they set a major requirement for security, privacy and trust management in a systematic manner. The chapter suggests Federated Identity Management and a single sign on framework in order to control access to patient data, as well as an auditing and reporting mechanism in order to validate and ensure compliance to security policies.

The ninth chapter, which is entitled *Certification and Security Issues in Biomedical Grid Portals: The GRISSOM Case Study*, discusses certification and security issues in biomedical grid portals and presents the security infrastructure of GRISSOM (Grids for In Silico Systems biology and Medicine) platform. GRISSOM consists of a web-based portal and a Web Service that enables statistical data analysis over a grid infrastructure. The chapter presents the security infrastructure that manages user authentication and access issues and offers data encryption, Grid secure access and Web Service Security.

Chapter ten, *Health 2.0 and Medicine 2.0: Safety, Ownership and Privacy Issues*, examines security of health related web applications under the collaborative prism of Medicine 2.0 and Health 2.0. The virtual interactions between patients and health professionals raise concerns about disintermediation and magnify the need for privacy and information security. The chapter considers the key debates that occur in the literature with respect to the terms Medicine 2.0 and Health 2.0 and examines all potential solutions to security and privacy issues from a patient-centered aspect.

The eleventh chapter, entitled *Securing and Prioritizing Health Information in TETRA Networks*, studies the issues of collecting and transferring patient information using mobile devices. The study refers to TETRA networks and examines how simply a healthcare professional can collect physiological data from mobile and/or remote patients and how securely and reliably health information can be transferred from emergency places to hospitals. The chapter gives an overview of the TETRA technology and analyses the characteristics of TETRA calls.

Chapter twelve, *Online Advertising in Relation to Medicinal Products and Health Related Services: Data & Consumer Protection Issues*, examines several issues of online advertising in relation to medicinal

products and health related services. The chapter clearly shows that the marketing of medicinal products over the internet puts consumers at a number of risks related to both their privacy and their health and studies whether the existing EU legislation can efficiently protect the individual, who may be induced to disclose his/her health related information.

In chapter thirteen, *Password Sharing and How to Reduce It*, authors present a cross sectional case study of how healthcare professionals actually deal with password authentication in typical real world scenarios. The chapter compares the professionals' actual practice with what they feel about password sharing and what are the most frequent problems associated with it and suggests how to solve or minimize some of these problems by using both technological and social cultural mechanisms.

Finally, chapter fourteen, *Behavioral Security: Investigating the Attitude of Nursing Students Toward Security Concepts and Practices*, presents a case study on behavioral factors toward the applicability of security measures and practices in healthcare applications and investigates human attitudes in regards to security consciousness and familiarity. The study empirically assesses the intention of undergraduate nursing students to apply security concepts and practices and concludes that the perceived benefits, the general security orientation and self-efficacy of nursing students in applying security concepts and practices is more significant than a series of other constructs.

CONCLUSION

The main aim of this book is to enlighten the path for building secure and trustful healthcare applications for the web, which is expected to serve patients' and practitioners' aims. This holistic approach comprises several actions, such as:

- To alert patients and practitioners in regards to security issues, and more specifically,
- To raise the level of security awareness of: a) IT professionals, who develop, maintain or contribute to health related communities, b) patients that reveal their privacy to a doctor over the web and make use of medical advices shared by other patients, c) medical professionals that use web based applications and may not understand the special issues that arise when accessing medical data across huge and potentially unsecured computer networks, d) pharmacists that use the World Wide Web to acquire medical information or pharmaceutical products or to supply pharmaceutical services of their own by means of internet pharmacies,
- To propose a set of technologies, which can under circumstances ensure that patients and medical professionals benefit from using community services while minimizing the risk of phishers, spammers, hackers and crackers exploiting potential security holes,
- To form a methodology for certifying the validity of exchangeable medical data, exchanging parties and the exchange process.
- To review the certification and security procedures through collaboration, to identify open threats and emerging needs and to provide solutions.
- To cover as many security and certification issues as possible and provide practical solutions and case study applications.
- To identify the need for frequently revisable security plans and periodical risk assessments in order to update the overall security of health information systems.

This holistic solution can be summarized to a flexible security management system, which complies with standards, takes into account all the restrictions imposed by law and continuously evolves and strengthens against potential risks. The gains from a certified security management solution are multifold both for patients and medical professionals: (1) the availability of healthcare information is valuable for the effective operation of healthcare organizations, (2) the protection of the personal and healthcare information, promotes the trust among patients and the healthcare professionals, (3) minimizing risk from the medical law point of view protects healthcare enterprises and organizations from legal sanctions – penalties and reduces negotiation overhead between the healthcare organization and the patient.

This book provides a novel aspect of security of medical applications, which covers both security and certification. It touches several legal and ethical issues that relate to the use of health information and introduces a new perspective on the security of healthcare information systems which relates to the acceptance of security policies and technologies by the medical community members. It is an excellent source of comprehensive knowledge and literature on the topic of certification and security in e-health applications and we hope that readers will find it useful when endeavoring in their line of work.

Anargyros Chryssanthou
Hellenic Data Protection Authority, Greece

Ioannis Apostolakis
National School of Public Health, Greece

Iraklis Varlamis
Harokopio University of Athens, Greece

Acknowledgment

First of all, we would like to thank the Editorial Board Members, authors, readers, and reviewers for their great help and support in this book and we look forward to collaborate again in future projects. Special thanks go to Dr. Anastasia Kastania and Dr. Athina Lazakidou for their useful advices concerning the preparation of this book.

Finally, we would like to thank IGI Global for giving us the opportunity to publish this work and for supporting us throughout the whole process.

Anargyros Chryssanthou
Hellenic Data Protection Authority, Greece

Ioannis Apostolakis
National School of Public Health, Greece

Iraklis Varlamis
Harokopio University of Athens, Greece