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.