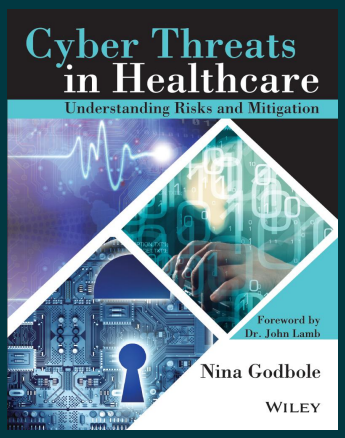
WILEY



Cyber Threats in Healthcare: Understanding Risks and Mitigation

By Nina Godbole

Paperback 9788126560127 ₹1,129.00

Description

Cyber Threats in Healthcare: Understanding Risks and Mitigation deals with the key areas of healthcare cyber security. This book talks about the importance of securing private medical data of people, which is deployed in the Cloud, a topic that has been neglected until now. This book is unique as it is for the first time that the issues of cyber risk in the healthcare sector and the associated security challenges are discussed. The increased use of IT and portable mobile devices in the healthcare industry has increased the need for cyber security, and these areas are comprehensively covered in the chapters. The book also discusses the facets of modern technology and the related security concerns.

Appendix

Further-Readings

About the Author

Nina Godbole

Nina Godbole has wide experience in the IT industry – SW development, system analysis and design, software testing, business development and support services, training, quality management, operations management, and the design and implementation of computer-based MIS applications. The author was instrumental in preparing IT perspective plans for client organisations as well as BPR initiatives

Table of Contents

1 Healthcare Sector in Global Context

1.1 Introduction

1.2 The Use of IT and Portable Mobile Devices in Healthcare

2 Healthcare Sector in India

2.1 Introduction

2.2 Indian Healthcare Sector under Transformation

2.3 The Structure and Organisation of the Healthcare System Delivery in India

2.4 Medical Devices Industry in India

2.5 India’s Private Health Sector: The Regulatory Situation

2.6 Protected Health Data and Its Privacy in India

2.7 Telemedicine Practice in India

3 ICT and AI in Healthcare
3.1 Introduction
3.2 HIMS/HMIS/HIT in Healthcare
3.3 Health Information Exchange: What and why
3.4 Structure and Objectives of HIMS and HMIS
3.5 HIMS: Benefits
3.6 ICT Benefits to Healthcare Industry
3.7 Clinical Decision Support Systems in Healthcare
3.8 Artificial Intelligence in Healthcare
4 EHR and EMR
4.1 Introduction
4.2 Electronic Health Records
4.3 EHR: Adoption, Benefits and Risks
4.4 Electronic Medical Records
4.5 EHRs and EMRs: Security and Privacy Implications
5 Information Security and Data Privacy in Healthcare
5.1 Introduction
5.2 Information Security in Healthcare: Key Concepts
5.3 Security of Healthcare Data Transmission
5.4 Understanding ‘Data Privacy’ and Its Importance in Healthcare Context
5.5 Protected/Personal Health Information and Its Importance
5.6 Medical Data and Access Control
5.7 B.Y.O.D. and Its Importance
5.8 Privacy Concerns with Context-Aware Applications and Intelligent (Software) Agents Used in Healthcare
5.9 Privacy Concerns with the Use of RFID Technology in Healthcare
5.10 Awareness of Data Privacy in Healthcare: Current Status
6 Big Data and Cloud Technologies in Healthcare
6.1 Introduction
6.2 Understanding Cloud Technologies
6.3 Benefits of ‘Cloud’ to Healthcare
6.4 Big Data: The Evolutionary Journey
6.5 Healthcare Analytics in Indian Healthcare
6.6 Data-Related Issues and Challenges in Healthcare
6.7 Big Data Usage in Healthcare: Limitations and Obstacles
6.8 Concept and Practice of ‘Meaningful Use’ and Its Implications for Healthcare ‘Privacy’
7 Cyber Threats to Healthcare Information
7.1 Introduction
7.2 Cyber Space and Cyber Criminals

7.3 Protected Health Information: Characteristics, Protection and Access

7.4 Perceived Value of Healthcare Industry’s Data: Cyber Criminals’ Perspective

7.5 Cyber Threats to Healthcare Sector: From Where They Come

7.6 Financial Implications of Cyber Threats to Healthcare

7.7 Healthcare Data Breaches: Indian Scenario

7.8 Healthcare Data and Mobile Devices

8 IoT: The New Dimension of Cyber Threats to Healthcare Data

8.1 Introduction

8.2 The Rise of IoT

8.3 IoT: The New ‘Threat Scape’ to Healthcare Information

8.4 IoT and Wearable Medical Devices

8.5 IoT-Connected Mobile Devices: Benefits and Security Threats to Healthcare Data

8.6 Threats to Patient Safety and IoT-connected Medical Devices

8.7 Medjacking: The Hijacking of IoT-connected Medical Devices

9 Semantic Web for Healthcare and Data Security Concerns

9.1 Introduction to the Semantic Web

9.2 Current Web: The Limitation from Healthcare Perspective

9.3 The Need for Semantic Web Technologies

9.4 Semantic Web in the Context of Continuous Care and Chronic Diseases

9.5 Semantic Web, Healthcare Ontologies, CDSS, Interoperability and Sharing of Medical Data: Understanding the Relation

9.6 Privacy and Security in the Semantic Web

9.7 Semantic Web and Ontologies: Implications for Healthcare

10 Regulatory Environment in Healthcare Industry

10.1 Introduction

10.2 HIPAA, HITECH and HL7: An Overview

10.3 The Personal Health Information Protection Act

10.4 Regulations for Safety and Security of Medical Devices

10.5 ISO Standards Applicable to Healthcare Sector

10.6 Other Supporting ISO Standards Applicable to Healthcare Sector

11 Patient Privacy Protection and Healthcare Data Security: Indian Regulatory Scenario

11.1 Introduction

11.2 Healthcare Services Planning: A Precursor to Regulatory Controls

11.3 Indian Healthcare Sector and Existing Regulations: An Overview

11.4 Indian Standards for EHRs and Their Adoption

11.5 Data Privacy Frameworks and Laws in India

11.5.3 The Future for Sector-Specific Laws and Regulatory Guidance in India

11.6 HDPSA: The Indian Version of HIPAA

11.7 DISHA: The New Direction to India’s Path Towards Healthcare Data Privacy and Security
11.8 ‘Data Breach’ Notification Requirements in India
11.9 Protection of Medical Devices to Prevent Security Threats: Do Laws Exist in India?
11.10 Right to Patient Privacy: Indian Case Laws
11.11 The Regulatory Landscape for the Indian Pharma Sector
11.12 Laws Applicable in India for Commissioning of Hospitals and Patients’ Rights
12 Healthcare Cyber Risks Mitigation: Best Practices
12.1 Introduction
12.2 Risk Mitigation Strategies in the Face of Cyber Threats to Healthcare Data
12.3 Healthcare Information Systems Risk Management Best Practices
12.4 Creating an Effective Plan for Healthcare Cyber security Risk Management
12.5 Mobile Device Management Best Practices for Healthcare
12.6 Data Obfuscation, Data Encryption, Data De-identification/Data Anonymisation and Tokenisation of Data
12.7 The Use of ‘Blockchain’ Technology
12.8 Biometric Controls to Protect Healthcare Data from Bioterrorism
12.9 Establishing B.Y.O.D. Policy: A Best Practice to Protect Healthcare Data
12.10 Precautions with the Use of Intelligent (Software) Agents in Healthcare
12.11 Physical Security Controls as Best Practice
12.12 HR Best Practices for Hospitals and Other Healthcare Organisations
12.13 Security Audits and Privacy Audits
Summary
Review Questions
Mini Project 1
Mini Project 2
Index

To purchase this product, please visit:
https://www.wileyindia.com/cyber-threats-in-healthcare-understanding-risks-and-mitigation.html

Scan to buy