

IT SECURITY IN THE HEALTHCARE INDUSTRY

“Protecting Patient Data, Securing Health Systems, and Ensuring Regulatory Compliance.”

Schedule

Venue	Fees
In-House	ASK FOR THE QUOTATION

► Available delivery methods: In-House Training

Introduction

As healthcare becomes increasingly digital, it faces rising threats from cyberattacks, ransomware, and data breaches. This course provides healthcare IT professionals, administrators, and security managers with the knowledge and tools to defend against threats, ensure compliance with regulations like HIPAA and GDPR, and build resilient digital health ecosystems. Participants will explore real-world case studies, adopt best practices, and develop a comprehensive understanding of IT security in a clinical and organizational context.

Objectives

By the end of this training, participants will be able to:

- Understand the unique cybersecurity challenges in healthcare
- Protect electronic health records (EHR) and medical devices from cyber threats
- Manage compliance with data protection regulations (HIPAA, GDPR, HITECH)
- Develop and implement healthcare-specific information security policies
- Respond to security incidents and minimize downtime

Why Attend

This course bridges the gap between IT security principles and their healthcare-specific applications, helping professionals safeguard patient data and clinical operations from ever-evolving cyber risks.

Target Audience

- Healthcare IT managers and systems administrators
- Hospital CIOs and CISOs
- Risk, privacy, and compliance officers
- Clinical informatics specialists
- Healthcare service providers using digital platforms

Individual Benefits

- Gain hands-on knowledge in securing health data and systems
- Enhance professional credentials in healthcare cybersecurity
- Improve response to audits and minimize risk of breaches
- Strengthen decision-making on IT investments and digital transformation

Organizational Benefits

- Mitigate risk of data breaches and financial penalties
- Enhance patient trust and data confidentiality
- Ensure regulatory readiness and audit resilience
- Protect healthcare operations and business continuity

Instructional Methodology

- Case-based learning with healthcare data breach scenarios
- Simulated threat exercises and incident response planning
- Compliance documentation workshops
- Expert-led lectures with healthcare IT tools and systems

Course Outline

DETAILED 5-DAY COURSE OUTLINE (CUSTOMIZABLE)

Training Hours: 7:30 AM – 3:30 PM

Daily Format: 3–4 Learning Modules | Coffee Breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Introduction to Healthcare Cybersecurity

Module 1: Digital Health Trends & Security Impacts (07:30 – 09:30)

Module 2: Overview of EHR, Telemedicine, PACS & IoMT Threats (09:45 – 11:15)

Module 3: Common Healthcare Attack Vectors (Phishing, Malware, Ransomware) (11:30 – 01:00)

Module 4: Real-World Case Studies of Health Sector Data Breaches (02:00 – 03:30)

Day 2: Security Risk Management & Governance

Module 1: Conducting Risk Assessments in Hospitals (07:30 – 09:30)

Module 2: Business Continuity & Incident Management Planning (09:45 – 11:15)

Module 3: Security Governance Models for Healthcare IT (11:30 – 01:00)

Module 4: Policy Development: Access, Authentication & Data Retention (02:00 – 03:30)

Day 3: Regulatory Compliance in Healthcare

Module 1: HIPAA, HITECH, GDPR & Local Health Data Regulations (07:30 – 09:30)

Module 2: Preparing for Compliance Audits & Data Classification (09:45 – 11:15)

Module 3: Documentation of Breach Notification & Consent Protocols (11:30 – 01:00)

Module 4: Workshop: Drafting a Healthcare IT Compliance Framework (02:00 – 03:30)

Day 4: Securing Infrastructure & Medical Devices

Module 1: Network Security in Clinical Environments (07:30 – 09:30)

Module 2: Endpoint Security & BYOD in Healthcare (09:45 – 11:15)

Module 3: Protecting IoMT & Medical Devices from Exploits (11:30 – 01:00)

Module 4: Incident Response: Creating a Cyberattack Playbook (02:00 – 03:30)

Day 5: Strategic Security Planning & Emerging Technologies

Module 1: Cybersecurity in AI, Telemedicine & Health Apps (07:30 – 09:30)

Module 2: Cloud Security & Data Encryption in Health Systems (09:45 – 11:15)

Module 3: Final Exam & Threat Simulation Exercise (11:30 – 01:00)

Module 4: Certification Wrap-Up & Action Plan Development (02:00 – 03:30)

Certification

Participants who complete all modules and assessments will receive a **Certificate in IT Security in the Healthcare Industry**, demonstrating their proficiency in protecting digital health infrastructures and complying with healthcare-specific cybersecurity standards.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: +601116373203	EMAIL: info@mawaevents.net
---	----------------------------------	--

© Material published by MAWA Events shown here is copyrighted. All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.