# Cybersecurity in Health Systems Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Public Health | **Duration** | 5 Days |
| **Base Fee** | $1,500 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

Cybersecurity in health systems is now a critical global priority as healthcare organizations increasingly depend on digital health records, telemedicine platforms, IoT medical devices, and cloud-based hospital systems. With rising threats such as ransomware attacks, data breaches, phishing campaigns, and insider threats, protecting patient data and ensuring system resilience has become essential for safe and reliable healthcare delivery. Cybersecurity in Health Systems Training Course is designed to equip learners with advanced competencies in healthcare cybersecurity frameworks, risk management, compliance standards (HIPAA/GDPR-like regulations), and threat mitigation strategies tailored specifically for clinical environments.

The course provides a comprehensive understanding of how to secure Electronic Health Records (EHR), Hospital Information Systems (HIS), Medical IoT (IoMT), and digital diagnostic platforms. Participants will explore real-world attack scenarios, incident response strategies, and emerging technologies such as AI-driven cybersecurity, zero-trust architecture, blockchain in healthcare security, and cloud security for health systems. The training emphasizes hands-on application, ensuring professionals can defend critical healthcare infrastructure against evolving cyber threats while maintaining patient safety and operational continuity.

## Programme Curriculum

**Cybersecurity in Health Systems Training Course**

**Introduction**

Cybersecurity in health systems is now a critical global priority as healthcare organizations increasingly depend on digital health records, telemedicine platforms, IoT medical devices, and cloud-based hospital systems. With rising threats such as ransomware attacks, data breaches, phishing campaigns, and insider threats, protecting patient data and ensuring system resilience has become essential for safe and reliable healthcare delivery.

Cybersecurity in Health Systems Training Course is designed to equip learners with advanced competencies in healthcare cybersecurity frameworks, risk management, compliance standards (HIPAA/GDPR-like regulations), and threat mitigation strategies tailored specifically for clinical environments.

The course provides a comprehensive understanding of how to secure Electronic Health Records (EHR), Hospital Information Systems (HIS), Medical IoT (IoMT), and digital diagnostic platforms. Participants will explore real-world attack scenarios, incident response strategies, and emerging technologies such as AI-driven cybersecurity, zero-trust architecture, blockchain in healthcare security, and cloud security for health systems. The training emphasizes hands-on application, ensuring professionals can defend critical healthcare infrastructure against evolving cyber threats while maintaining patient safety and operational continuity.

**Course Duration**

5 days

**Course Objectives**

1. Master Healthcare Cybersecurity Frameworks & Compliance Standards
2. Understand Ransomware Defense in Hospital Systems
3. Implement Zero Trust Security Architecture in Healthcare IT
4. Strengthen Electronic Health Records (EHR) Protection Strategies
5. Detect and mitigate Phishing & Social Engineering Attacks
6. Apply Medical IoT (IoMT) Security Controls
7. Develop Incident Response & Cyber Crisis Management Plans
8. Ensure Cloud Security in Digital Health Systems
9. Analyze Healthcare Data Privacy & Protection Laws
10. Build Cyber Risk Assessment Models for Hospitals
11. Use AI & Machine Learning in Threat Detection
12. Secure Telemedicine and Remote Patient Monitoring Systems
13. Design Resilient Healthcare Cyber Defense Infrastructure

**Target Audience**

- Healthcare IT Administrators
- Hospital Network Engineers
- Cybersecurity Analysts in Healthcare
- Medical Records & Data Management Officers
- Health Informatics Professionals
- Clinical Operations Managers
- Government Health ICT Policy Makers
- Cybersecurity Students & Researchers

**Course Modules**

**Module 1: Foundations of Healthcare Cybersecurity**

- Overview of healthcare digital ecosystems
- Key cybersecurity threats in hospitals
- Types of cyberattacks in healthcare systems
- Security principles: CIA triad in healthcare
- Introduction to compliance frameworks

- **Case Study:** 2017 WannaCry attack on healthcare systems

**Module 2: Healthcare Risk Management & Compliance**

- Risk identification in clinical systems
- HIPAA/GDPR-aligned data protection models
- Security auditing in healthcare institutions
- Policy development for cyber governance
- Third-party vendor risk management
- **Case Study:** Hospital vendor breach leading to patient data leak

**Module 3: Electronic Health Records (EHR) Security**

- EHR architecture vulnerabilities
- Access control mechanisms (RBAC, ABAC)
- Encryption techniques for patient data
- Secure data sharing protocols
- Audit trails and monitoring systems
- **Case Study:** Unauthorized EHR access incident in a hospital network

**Module 4: Medical IoT (IoMT) Security**

- Security challenges in connected medical devices
- Device authentication mechanisms
- Firmware and patch management
- Network segmentation for IoMT
- Real-time monitoring systems
- **Case Study:** Cyberattack on insulin pump vulnerabilities

**Module 5: Cloud Security in Healthcare Systems**

- Cloud deployment models in healthcare
- Data encryption in cloud storage
- Identity and access management (IAM)
- Secure APIs in healthcare cloud apps
- Disaster recovery strategies
- **Case Study:** Misconfigured cloud storage exposing patient records

**Module 6: Threat Detection & Incident Response**

- Security Information and Event Management (SIEM)
- Intrusion detection systems (IDS/IPS)
- Threat intelligence frameworks
- Incident response lifecycle
- Digital forensics in healthcare
- **Case Study:** Response to hospital ransomware outbreak

**Module 7: Advanced Cybersecurity Technologies**

- Artificial Intelligence in threat detection
- Blockchain for healthcare data integrity
- Behavioral analytics for anomaly detection

- Zero Trust Architecture implementation
- Automation in cybersecurity operations
- **Case Study:** AI-based early detection of phishing in hospital network

**Module 8: Telemedicine & Remote Health Security**

- Security risks in telehealth platforms
- Secure video consultation systems
- Mobile health app protection
- Patient authentication systems
- Secure data transmission protocols
- **Case Study:** Breach in telemedicine platform exposing patient consultations

## Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.org or call** *+254769199797*

***Certification***

*Upon successful completion of this training, participants will be issued with a globally- recognized certificate.*

***Tailor-Made Course***

*We also offer tailor-made courses based on your needs.*

**Key Notes**

**a.** The participant must be conversant with English.

**b.** Upon completion of training the participant will be issued with an Authorized Training Certificate

**c.** Course duration is flexible and the contents can be modified to fit any number of days.

**d.** The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

**e.** One-year post-training support Consultation and Coaching provided after the course.

**f.** Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

## Upcoming Scheduled Sessions

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **23 Nov 2026** | 27 Nov 2026 | Online | $1,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $1,500 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $3,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $3,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $4,500 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |
| **23 Nov 2026** | 27 Nov 2026 | Physical | $6,000 |

Ready to enroll or request a customized program? Book online or contact us:

**Register Online Now**

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com