Health Information Technology Security (HITS) Training Course

Professional Development Training Course Outline

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

Course Introduction

In the age of Digital Transformation, the healthcare sector is a prime target for increasingly sophisticated Cyber Threats. The convergence of sensitive Electronic Health Records (EHR), interconnected Internet of Medical Things (IoMT) devices, and expanding Telehealth platforms has created a vast, complex Attack Surface. Health Information Technology Security (HITS) Training Course is essential for organizations to uphold Patient Privacy and safeguard critical systems. A single Data Breach often resulting from a lack of Security Awareness or failure to implement current Zero Trust architectures can lead to massive financial penalties, significant operational disruption, and catastrophic loss of patient trust.

This comprehensive Health Information Technology Security (HITS) course provides an immersive, Hands-on Training experience focused on implementing and managing robust security controls. Participants will master the intricacies of regulatory compliance, including the HIPAA Security Rule and HITECH Act, while gaining practical skills in Threat Modeling, Vulnerability Management, and Incident Response. We move beyond theoretical concepts to focus on Real-World Case Studies and defensive strategies, ensuring graduates are equipped to build a Cyber-Resilient Healthcare Ecosystem and become indispensable Healthcare Cybersecurity Professionals.

Programme Curriculum

Health Information Technology Security (HITS) Training Course

Introduction

In the age of Digital Transformation, the healthcare sector is a prime target for increasingly sophisticated Cyber Threats. The convergence of sensitive Electronic Health Records (EHR), interconnected Internet of Medical Things (IoMT) devices, and expanding Telehealth platforms has created a vast, complex Attack Surface. Health Information Technology Security (HITS) Training Course is essential for organizations to uphold Patient Privacy

and safeguard critical systems. A single Data Breach often resulting from a lack of Security Awareness or failure to implement current Zero Trust architectures can lead to massive financial penalties, significant operational disruption, and catastrophic loss of patient trust.

This comprehensive Health Information Technology Security (HITS) course provides an immersive, Hands-on Training experience focused on implementing and managing robust security controls. Participants will master the intricacies of regulatory compliance, including the HIPAA Security Rule and HITECH Act, while gaining practical skills in Threat Modeling, Vulnerability Management, and Incident Response. We move beyond theoretical concepts to focus on Real-World Case Studies and defensive strategies, ensuring graduates are equipped to build a Cyber-Resilient Healthcare Ecosystem and become indispensable Healthcare Cybersecurity Professionals.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Define and enforce the HIPAA Security Rule and HITECH Act requirements for ePHI protection.
2. Perform a comprehensive Risk Assessment and Threat Modeling specifically for clinical environments.
3. Implement and manage Zero Trust Architecture (ZTA) principles across healthcare networks.
4. Apply Network Segmentation strategies to isolate IoMT/Medical Devices and critical systems.
5. Develop and execute robust Incident Response Plans (IRP) for Ransomware Attacks.
6. Master Vulnerability Management and Patch Management processes for clinical IT systems.
7. Design secure Cloud Computing strategies for healthcare data
8. Recognize, mitigate, and prevent common Social Engineering and Phishing Attacks targeting healthcare staff.
9. Secure **Telehealth** and **Remote Access** infrastructure using modern **MFA** and VPN solutions.
10. Establish effective Business Associate Agreements (BAAs) and manage Third-Party Risk in the supply chain.
11. Implement Data Loss Prevention (DLP) and Encryption standards for data at rest and in transit.
12. Conduct Security Awareness Training programs to foster a Cybersecurity Culture across the organization.
13. Utilize Security Information and Event Management (SIEM) tools for continuous Threat Detection and Compliance Monitoring.

Target Audience

1. HIPAA Security and Privacy Officers
2. Health IT (HIT) Managers/Administrators
3. Clinical Engineers and Biomedical Technicians.
4. Information Security Analysts/Specialists.
5. Healthcare Consultants and Auditors.
6. EHR System Developers and Integrators
7. C-Suite Executives.
8. IT/Security Business Associates and third-party vendors handling ePHI.

Course Modules

Module 1: Healthcare Regulatory Foundations (GRC)

- In-depth analysis of the HIPAA Security Rule and its Administrative, Physical, and Technical Safeguards.
- Understanding the HITECH Act and the Omnibus Rule's impact on breach liability and enforcement.
- Defining and securing ePHI across the full data lifecycle
- Mandatory documentation.
- Case Study: Anthem, Inc. Breach (2015).

Module 2: Risk Management and Threat Modeling

- Conducting a formal, comprehensive HIPAA Security Risk Assessment using NIST standards
- Identifying and prioritizing common Healthcare Threat Vectors
- Developing mitigation strategies and managing the Risk Register to achieve a reasonable and appropriate security posture.
- Calculating the probability and impact of risks to determine overall organizational exposure.
- Case Study: Change Healthcare Cyberattack (2024).

Module 3: Network and Infrastructure Security (IoMT Focus)

- Implementing Zero Trust Architecture in a hospital setting
- Advanced Network Segmentation strategies for isolating the IoMT network from the main EHR network.
- Securing remote access for clinicians and vendors via Zero Trust Network Access and robust VPNs.
- Hardening critical infrastructure: Firewalls, Intrusion Detection/Prevention Systems, and secure configuration management.
- Case Study: WannaCry Ransomware (2017).

Module 4: Identity, Access, and Cloud Security

- Designing and deploying robust Identity and Access Management systems, including Multi-Factor Authentication
- Implementing Principle of Least Privilege for all users, especially those with access to ePHI.
- Securing Cloud Computing environments and understanding the Shared Responsibility Model in healthcare.
- Administering security for Telehealth platforms and remote patient monitoring systems.
- Case Study: Blackbaud Ransomware Incident (2020).

Module 5: Incident Response and Business Continuity

- Creating a robust Healthcare Incident Response Plan with defined roles, communication protocols, and legal counsel involvement.
- Simulating and conducting Tabletop Exercises for common scenarios
- Implementing Disaster Recovery and Business Continuity Planning to maintain essential clinical operations during an attack.
- Collecting and preserving Digital Forensic evidence post-incident for regulatory and legal review.
- Case Study: Hospital System Ransomware Attack

Module 6: Threat Detection and Vulnerability Management

- Managing the lifecycle of Vulnerabilities in HITS.
- Utilizing Security Information and Event Management and Security Orchestration, Automation, and Response tools for real-time monitoring.
- Conducting Penetration Testing and Red Teaming exercises focused on EHR and IoMT environments.

- Understanding the role of Threat Intelligence in predicting and preparing for targeted attacks.
- Case Study: Equifax Breach (2017).

Module 7: Data Protection and Application Security

- Implementing Encryption best practices for ePHI.
- Deploying Data Loss Prevention tools to monitor and block unauthorized exfiltration of sensitive data.
- Introduction to secure software development practices for in-house clinical applications.
- Securing patient portals and web applications against common attacks.
- Case Study: Premera Blue Cross Breach (2014).

Module 8: The Human Factor and Security Awareness

- Designing and implementing mandatory, effective Security Awareness Training tailored for clinical and administrative staff.
- Identifying and mitigating Insider Threats.
- Advanced techniques for defending against Social Engineering, Phishing, and Vishing attacks.
- Developing strong Acceptable Use Policies for mobile devices and remote work access.
- Case Study: Tennessee Hospital System Phishing Attack.

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