JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

AI in Healthcare Cybersecurity Training Course

7 – 11 March 2027
Kuala Lumpur

jupiterprime.uk
info@jupiterprime.uk
Registered in the United Kingdom and Saudi Arabia

AI in Healthcare Cybersecurity Training Course

Ref: 92_2311 **Date:** 7 – 11 March 2027 **Location:** Kuala Lumpur **Fees:** 4900 GBP

AI in Healthcare Cybersecurity is a 1-week training course for hospital IT security managers, clinical systems leads, health information officers and risk managers, ending with a healthcare AI security response plan. Ransomware crews target hospitals because downtime endangers patients, while connected infusion pumps, imaging scanners and diagnostic algorithms widen the attack surface every month. Jupiter Prime Training runs this AI in Healthcare Cybersecurity course.

Why AI in Healthcare Cybersecurity Matters Now

Attackers now use automation to find unpatched clinical systems and craft phishing aimed at ward staff. Hospitals connect more bedside devices, laboratory analysers and cloud electronic health record services, many of them hard to patch. Clinicians and patients expect diverted ambulances, cancelled surgery and leaked records to be rare. A hospital that handles this well detects intrusions early and keeps care running; one that handles it badly falls back to paper, delays treatment and loses patient trust. The course draws on ISO/IEC 42001 for AI management systems and the NIST AI Risk Management Framework NIST AI RMF for securing clinical models.

Who Gains Most from AI in Healthcare Cybersecurity

- Security leads who run hospital monitoring, incident handling and threat intelligence
- Clinical systems owners who keep electronic records, imaging and laboratory platforms available
- Biomedical engineering leads who inventory and patch connected medical devices
- Information officers who decide who may access patient records and why
- Risk leads who rate cyber exposure for the executive board and insurers

A hospital group or health authority gains most when its security, clinical systems and biomedical engineering leads attend together and rehearse one ransomware scenario end to end.

AI in Healthcare Cybersecurity Capabilities

Participants read alert queues, device inventories and record access logs from clinical settings, and decide where machine learning raises an alarm and where an analyst confirms it.

- Assess anomaly detection on clinical networks against false alarm tolerance — security operations
- Design ransomware defence and downtime procedures that keep wards running — clinical directors
- Specify segmentation and patch priorities for connected medical devices — biomedical engineering
- Apply access monitoring that flags unusual viewing of patient records — information officers
- Test clinical AI models for poisoning, evasion and manipulated inputs — model owners
- Communicate cyber exposure and recovery readiness to boards and insurers — risk committees

Key AI in Healthcare Cybersecurity Terms

- Anomaly detection — models that learn normal network or user behaviour and flag departures signalling intrusion.
- Ransomware — malicious software that encrypts systems or records and demands payment, often after stealing copies.
- Internet of Medical Things — networked clinical devices such as infusion pumps, monitors and scanners that exchange data with hospital systems.
- Network segmentation — dividing a hospital network into zones so a compromise in one area cannot spread freely to clinical systems.
- Adversarial attack — deliberately crafted inputs that cause a model to misclassify, such as altered images fooling a diagnostic algorithm.
- Data poisoning — corrupting training records so a model learns wrong patterns that an attacker can later exploit.

AI in Healthcare Cybersecurity Day by Day

Day 1: The Clinical Threat Landscape

- Hospital Attack Surface Mapping — Records, Devices and Cloud Links
- Ransomware Case Studies From Hospitals and Laboratories — Patient Impact
- Attacker Use of Automation — Phishing and Vulnerability Discovery
- Clinical Downtime Dependencies — Which Services Fail First
- Security Operations Maturity Check — Monitoring, Staffing and Playbooks

Day 2: Machine Learning for Threat Detection

- Network Anomaly Detection — Baselines for Clinical Traffic
- User Behaviour Analytics — Unusual Record Access by Staff
- Alert Triage Automation — Ranking Incidents for Analysts
- Threat Intelligence Enrichment — Matching Indicators to Hospital Assets
- Detection Tuning — False Positives Versus Missed Intrusions

Day 3: Medical Devices and Patient Records

- Medical Device Inventory and Risk Scoring — Patch Priorities
- Network Segmentation for Bedside Devices — Containing Lateral Movement
- Electronic Health Record Access Controls — Least Privilege for Clinicians
- Backup and Recovery Design — Restoring Records After Encryption
- Supplier Security Clauses — Device Makers and Cloud Providers

Day 4: Securing Clinical AI Models

- Adversarial Attacks on Diagnostic Models — Altered Images and Signals
- Training Data Poisoning — Provenance Checks for Clinical Datasets
- Model Theft and Inversion — Protecting Weights and Patient Inputs
- NIST AI RMF Manage Function — Responses to Model Security Incidents
- ISO/IEC 42001 Controls — Ownership, Monitoring and Change Approval

Day 5: Practising the Healthcare AI Security Response Plan

- Attack Surface and Downtime Map From Day 1 — Starting Exposure
- Detection and Triage Rules From Day 2 — Alert Handling
- Device and Record Safeguards From Day 3 — Containment Choices
- Clinical Model Protections From Day 4 — Assurance Steps
- Healthcare AI Security Response Plan — Tabletop-Tested Version for Approval

Applying AI in Healthcare Cybersecurity After the Course

- Run a ransomware tabletop with ward managers and clinical systems owners and list services lacking a downtime procedure.
- Rank connected medical devices by exposure and agree segmentation for the ten highest-risk units with biomedical engineering.

AI in Healthcare Cybersecurity Questions FAQ

What is AI in healthcare cybersecurity and why does it matter now?

AI in healthcare cybersecurity is the use of machine learning to detect attacks on hospital systems and the protection of clinical AI models themselves. It matters now because ransomware disrupts patient care and connected devices widen exposure.

Which roles gain most from AI in healthcare cybersecurity training?

Hospital IT security managers, clinical systems leads, health information officers and risk managers gain most. Biomedical engineering leads also benefit, because they secure connected medical devices.

How does AI in healthcare cybersecurity differ from a general cybersecurity management course?

It focuses on clinical settings: bedside devices, patient records, care downtime and diagnostic models rather than office networks. You plan defences around patient safety as well as data protection.

What do you bring back from AI in healthcare cybersecurity training?

You bring back a healthcare AI security response plan. It sets detection rules, device and record safeguards, clinical model protections and downtime steps tested in a tabletop exercise.

AI in Healthcare Cybersecurity: The Way Forward

The healthcare AI security response plan informs the first decision: which detection rules and device segments go live before the next audit cycle. Security operations, clinical systems owners and biomedical engineers use it during incidents and drills. After the first tabletop or real alert, revisit the downtime procedures and the model protections, because attackers adapt quickly to new defences.