CONCEPT

Healthcare Cybersecurity: Hospital Systems, Medical Devices and Patient Data



Healthcare Cybersecurity: Hospital Systems, Medical Devices and Patient Data

Introduction:

Healthcare cybersecurity is a 1-week course for hospital IT, security, biomedical engineering, clinical informatics and health data protection teams that produces a Healthcare Cyber Risk Register and Clinical Downtime Playbook. Hospitals run on electronic health records, imaging archives, laboratory systems and connected medical devices, so a ransomware outage or data breach becomes a patient safety and confidentiality problem, not only an IT fault. Participants already support clinical systems at work and apply each method to case study material from several hospital types. CoreConcept Training Center delivers this healthcare cybersecurity course.

Course Objectives:

- Map a hospital's clinical systems, connected medical devices and patient data flows and rank their cyber exposure by clinical impact
- Apply IEC 80001-1 risk management to networks that carry medical devices and define segmentation zones for clinical systems
- Manage medical device security from procurement to retirement with manufacturers, using SBOM data, MDS2 forms and patch agreements
- Control identity, access and supplier connections in clinical workflows without delaying patient care
- Coordinate cyber incident response and clinical downtime procedures that keep wards, imaging, laboratory and pharmacy services running
- Build a Healthcare Cyber Risk Register and report cyber risk to hospital leadership in patient safety terms

Target Audience:

- Hospital IT infrastructure and application support teams responsible for EHR, PACS, laboratory and pharmacy systems
- Information security functions responsible for monitoring, vulnerability handling and incident response in clinical environments
- Biomedical and clinical engineering teams responsible for connected medical device inventory, maintenance and manufacturer liaison
- Clinical informatics teams responsible for system configuration, user access and clinical workflow design
- Health data protection and privacy functions responsible for patient record confidentiality and breach handling

Course Outline:

Day 1: Why Healthcare Is Targeted and the Clinical IT Landscape

- Healthcare Threat Profile and Motives Behind Patient Data Theft
- Clinical Application Map Covering EHR, PACS, LIS and Pharmacy
- Connected Medical Device and IoMT Asset Inventory Build
- Ransomware Impact Chain From Encrypted Servers to Diverted Ambulances
- Clinical Cyber Exposure Baseline Using a Current-State Checklist

Day 2: Healthcare Security Standards and Clinical Network Architecture

- IEC 80001-1 Risk Management for Medical IT Networks
- IEC 81001-5-1 Health Software Security Lifecycle Expectations
- ISO 27799 Information Security Controls for Health Organisations
- HL7 and DICOM Interface Security for Clinical Data Exchange
- Clinical Network Segmentation Zones for Devices, Imaging and Guests

Day 3: Medical Devices, Clinical Access and Patient Data Protection

- MDS2 Form Review and Security Clauses in Device Procurement
- SBOM Analysis for Medical Device Vulnerability Tracking
- Legacy Device Compensating Controls and Manufacturer Patch Coordination
- Clinical Identity Management for Shared Workstations and Tap-and-Go Login
- Patient Record Confidentiality Controls, Encryption and Access Audit Trails

Day 4: Supplier Risk, AI Monitoring, Incident Response and Clinical Downtime

- Third-Party Remote Access Rules for Device Manufacturers and Vendors
- AI-Assisted Anomaly Detection for Clinical Network Traffic
- Healthcare Incident Response Roles Linking Security, Clinical and Communications Teams
- Clinical Downtime Procedures With Paper Forms and Read-Only Records
- Clinician Security Awareness on Phishing Reports and Shared Credentials

Day 5: Case Study: Healthcare Cyber Risk Register and Downtime Playbook

- Case Hospital Briefing on Systems, Devices, Suppliers and Data Flows
- Healthcare Cyber Risk Register Build Using Clinical Impact Scoring
- Downtime Tabletop Exercise for a Ransomware Outage in Imaging
- Cyber Risk Dashboard and Reporting Pack for Hospital Leadership
- Clinical Downtime and Incident Playbook Completion and Peer Review

Skills You Will Gain:

- Clinical Asset Mapping
- Medical IT Network Risk Assessment
- Medical Device Security Management
- Clinical Access Governance
- Supplier Access Control
- Patient Data Confidentiality Protection
- Clinical Downtime Planning
- Healthcare Cyber Risk Reporting

Why Attend This Course:

- Return with a Healthcare Cyber Risk Register and Clinical Downtime Playbook for the hospital security steering committee and clinical leadership to adopt
- Decide which legacy medical devices to isolate, patch through the manufacturer or retire, and document the reason for each choice
- Avoid prolonged service disruption when clinical systems fail, because wards and diagnostic departments already know their downtime routines
- Brief clinicians and department colleagues on secure login, phishing reporting and patient data handling in their daily work

Conclusion:

Once participants return, the hospital security lead, clinical engineering head and data protection function can use the Healthcare Cyber Risk Register to decide where to invest first in segmentation, device replacement and access controls, while the Clinical Downtime Playbook gives ward and department managers a tested routine for keeping care running during an outage. Healthcare cybersecurity then becomes a standing item on leadership agendas rather than a reaction to incidents. After the first real downtime event or exercise, the register scores and playbook steps should be reviewed against what actually happened.