Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

PUBLIC HEALTH

Cybersecurity in Health Systems Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
5 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 22, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

Cybersecurity in Health Systems Training Course

Public Health • 5 Days Intensive • Accredited Certification

Course Overview

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.

Key Skills & Software Tools Covered

Data protection • Risk management • Cyber threat detection • Health information security

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
11 May 2026 – 15 May 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
11 May 2026 – 15 May 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
11 May 2026 – 15 May 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**
11 May 2026 – 15 May 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 110,000**
11 May 2026 – 15 May 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 110,000**
11 May 2026 – 15 May 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 110,000**
11 May 2026 – 15 May 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 110,000**
11 May 2026 – 15 May 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 110,000**
11 May 2026 – 15 May 2026	Accra	Classroom / 5d	**$4,000 USD / KES 110,000**
18 May 2026 – 22 May 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
18 May 2026 – 22 May 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
18 May 2026 – 22 May 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

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

- Master Healthcare Cybersecurity Frameworks & Compliance Standards
- Understand Ransomware Defense in Hospital Systems
- Implement Zero Trust Security Architecture in Healthcare IT
- Strengthen Electronic Health Records (EHR) Protection Strategies
- Detect and mitigate Phishing & Social Engineering Attacks
- Apply Medical IoT (IoMT) Security Controls
- Develop Incident Response & Cyber Crisis Management Plans
- Ensure Cloud Security in Digital Health Systems
- Analyze Healthcare Data Privacy & Protection Laws
- Build Cyber Risk Assessment Models for Hospitals
- Use AI & Machine Learning in Threat Detection
- Secure Telemedicine and Remote Patient Monitoring Systems
- 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@datastatresearch.org or call +254724527104

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 DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/cybersecurity-in-health-systems-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.