Training Course on Medical Device Forensics and eHealth Systems

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This specialized training course is meticulously designed for digital forensic investigators, cybersecurity professionals, healthcare IT specialists, and regulatory compliance officers operating within the rapidly expanding domain of medical device forensics and eHealth systems. As healthcare increasingly relies on interconnected medical devices, electronic health records (EHRs), telemedicine platforms, and other eHealth technologies, these systems become critical sources of digital evidence in cases ranging from medical malpractice and patient data breaches to device tampering and cyber-physical attacks impacting patient safety. Training Course on Medical Device Forensics and eHealth Systems provides the crucial knowledge and hands-on skills to acquire, preserve, analyze, and interpret digital artifacts from these sensitive and highly regulated environments.

The curriculum delves into the unique challenges posed by proprietary medical device operating systems, specialized communication protocols (e.g., DICOM, HL7), and the stringent regulatory landscape (e.g., HIPAA, GDPR, and specifically Kenya's Digital Health Act and Data Protection Act). Participants will gain practical experience in identifying relevant data sources, extracting patient data, device usage logs, firmware details, and audit trails, and understanding the interoperability complexities of modern eHealth ecosystems. The course emphasizes forensically sound methodologies and strict adherence to data privacy and legal admissibility standards, ensuring graduates are equipped to conduct thorough investigations, safeguard patient information, and contribute to the security and integrity of healthcare delivery in the digital age.

Programme Curriculum

Training Course on Medical Device Forensics and eHealth Systems

Introduction

This specialized training course is meticulously designed for digital forensic investigators, cybersecurity professionals, healthcare IT specialists, and regulatory compliance officers operating within the rapidly expanding domain of medical device forensics and eHealth systems. As healthcare increasingly relies on interconnected medical devices, electronic health records (EHRs), telemedicine platforms, and other eHealth technologies, these systems become critical sources of digital evidence in cases ranging from medical malpractice and patient data breaches to device tampering and cyber-physical attacks impacting patient safety. Training Course on Medical Device Forensics and eHealth Systems provides the crucial knowledge and hands-on skills to acquire, preserve, analyze, and interpret digital artifacts from these sensitive and highly regulated environments.

The curriculum delves into the unique challenges posed by proprietary medical device operating systems, specialized communication protocols (e.g., DICOM, HL7), and the stringent regulatory landscape (e.g., HIPAA, GDPR, and specifically Kenya's Digital Health Act and Data Protection Act). Participants will gain practical experience in identifying relevant data sources, extracting patient data, device usage logs, firmware details, and audit trails, and understanding the interoperability complexities of modern eHealth ecosystems. The course emphasizes forensically sound methodologies and strict adherence to data privacy and legal admissibility standards, ensuring graduates are equipped to conduct thorough investigations, safeguard patient information, and contribute to the security and integrity of healthcare delivery in the digital age.

Course Duration

5 Days

Course Objectives

1. Identify and categorize diverse medical device types (e.g., implanted, wearable, diagnostic, therapeutic) and their forensic characteristics.
2. Understand the architecture of eHealth systems, including EHRs, telemedicine platforms, and health information exchanges.
3. Perform forensically sound data acquisition from various medical devices, including embedded systems, network-connected devices, and associated storage.
4. Extract and analyze patient health data (PHI), including vital signs, treatment logs, diagnostic images, and historical records, from eHealth systems.
5. Interpret device usage logs, audit trails, and firmware data from medical devices to reconstruct events and user interactions.

6. Investigate cybersecurity incidents affecting medical devices and eHealth systems, including ransomware, data breaches, and unauthorized access.
7. Understand proprietary data formats and communication protocols (e.g., DICOM, HL7) common in healthcare environments.
8. Navigate interoperability challenges and trace data flows across integrated eHealth platforms.
9. Comply with relevant data privacy regulations such as Kenya's Data Protection Act 2019 and the Digital Health Act, when processing health data.
10. Identify vulnerabilities and attack surfaces unique to medical devices and eHealth infrastructure.
11. Reconstruct complex incident timelines by correlating evidence from medical devices, EHRs, and network logs.
12. Utilize specialized forensic tools and techniques for healthcare-specific data analysis and visualization.
13. Generate comprehensive forensic reports suitable for legal, regulatory, and internal organizational purposes in healthcare investigations.

Organizational Benefits

1. Enhanced Patient Safety: Identify and investigate incidents of device malfunction or tampering that could impact patient care.
2. Improved Data Security & Privacy: Strengthen the ability to detect and respond to breaches of sensitive Patient Health Information (PHI).
3. Reduced Compliance Risk: Ensure all forensic activities adhere to stringent healthcare regulations (e.g., Kenya Data Protection Act, Digital Health Act).
4. Strengthened Incident Response: Develop specialized capabilities for rapid response to cybersecurity incidents in healthcare environments.
5. Proactive Threat Mitigation: Understand medical device vulnerabilities to implement stronger preventative security measures.
6. Cost Savings: Reduce reliance on expensive external specialists for medical device and eHealth forensics.
7. Robust Litigation Support: Produce admissible and compelling evidence for medical malpractice, fraud, or cybersecurity-related legal cases.
8. Maintained Public Trust: Demonstrate a commitment to securing patient data and ensuring the integrity of healthcare technology.
9. Actionable Intelligence: Gain insights into attack vectors and data handling practices to improve overall healthcare cybersecurity posture.
10. Specialized Skill Development: Equip staff with highly sought-after expertise in a rapidly growing and critical forensic domain.

Target Participants

- Digital Forensic Examiners in Healthcare
- Healthcare Cybersecurity Analysts
- Hospital IT Security Teams
- Medical Device Manufacturers (Security & Post-Market Surveillance)
- Regulatory Compliance Officers (Healthcare)
- Clinical Engineers / Biomedical Technicians (with a security interest)
- Law Enforcement Agencies Investigating Healthcare Fraud/Malpractice
- Health Information Management (HIM) Professionals
- Internal Audit Teams in Healthcare Organizations
- Privacy Officers (Healthcare Sector)

Course Outline

Module 1: Introduction to Medical Device & eHealth Ecosystems (Healthcare Forensics Fundamentals)

- Overview of Connected Medical Devices (Implantable, Diagnostic, Therapeutic, Wearable)
- Introduction to Electronic Health Records (EHR) and Health Information Systems (HIS)
- Understanding Telemedicine, mHealth, and Digital Health Platforms
- Unique Forensic Challenges: Patient Safety, Data Sensitivity, Regulatory Compliance
- **Case Study**: Mapping the data flow of a connected infusion pump within a hospital network.

Module 2: Medical Device Data Acquisition & Preservation (Medical Device Data Extraction)

- Forensically Sound Acquisition from Embedded Medical Devices
- Data Extraction from Connected Medical Devices (USB, Network, Wireless)
- Challenges of Volatile Memory and Real-time Data Acquisition
- Tools and Techniques for Device Imaging and Data Preservation
- **Case Study**: Acquiring logs and configuration data from a diagnostic imaging machine.

Module 3: Electronic Health Records (EHR) & Clinical System Forensics (EHR Forensics)

- Architecture and Data Structures of Major EHR Systems (e.g., Epic, Cerner)
- Forensic Analysis of EHR Audit Trails and Access Logs
- Investigating Data Tampering, Unauthorized Access, and Patient Record Modifications
- Extracting Clinical Notes, Prescriptions, and Treatment Plans from EHRs
- **Case Study**: Tracing unauthorized access to a patient's medical record within an EHR system.

Module 4: Medical Device Data Artifact Analysis (Medical Device Data Analysis)

- Analysis of Device Usage Logs, Alarms, and Event Histories
- Interpreting Patient Physiological Data and Treatment Parameters (e.g., heart rate, dosage, glucose levels)
- Extracting Firmware Versions, Configuration Files, and Device Settings
- Analyzing Geotagged Medical Data (e.g., from ambulances, remote monitoring devices)
- **Case Study**: Analyzing insulin pump data logs to investigate a suspected overdose.

Module 5: Network & Communication Protocols in eHealth (eHealth Network Forensics)

- Understanding Medical Device Communication Protocols (DICOM, HL7, FHIR)
- Network Traffic Analysis for Medical Devices and eHealth Systems
- Identifying Insecure Communication Channels and Data Exfiltration Attempts
- Investigating Telemedicine Session Data and VoIP Communications
- **Case Study**: Intercepting and analyzing network traffic from a medical IoT device for suspicious activity.

Module 6: Cybersecurity Incidents in Healthcare Forensics (Healthcare Cyber Forensics)

- Common Threats: Ransomware, Phishing, Insider Threats, Medical Device Exploits
- Investigating Data Breaches and Unauthorized Access to PHI
- Responding to Cyber-Physical Attacks Impacting Medical Devices (e.g., pacemaker hacks)
- Role of Forensic Readiness in Healthcare Incident Response
- **Case Study**: Forensic investigation of a ransomware attack targeting a hospital's HIS.

Module 7: Regulatory Compliance & Data Privacy in Forensics (Healthcare Data Privacy)

- Understanding HIPAA, GDPR, and other relevant international healthcare regulations.
- Deep Dive into Kenya's **Data Protection Act 2019** and the **Digital Health Act** (on health data processing).
- Managing Sensitive Personal Data and Patient Consent in Forensic Investigations
- Legal and Ethical Considerations for Medical Device and eHealth Data Acquisition
- **Case Study**: Navigating the legal requirements for acquiring patient data from a medical device for a court case in Kenya.

Module 8: Reporting, Expert Testimony & Future Trends (Healthcare Forensic Reporting)

- Best Practices for Documenting Medical Device and eHealth Forensic Examinations
- Crafting Comprehensive Forensic Reports for Regulatory Bodies, Legal Teams, and Internal Stakeholders
- Presenting Complex Technical Findings in Medical Malpractice or Product Liability Cases
- Emerging Technologies: AI in Healthcare, Connected Hospitals, Quantum Computing and their Forensic Implications
- **Case Study**: Preparing a mock expert witness report for a medical device malfunction leading to patient harm.

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 *+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 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
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100

Start Date	End Date	Location	Price
28 Sep 2026	02 Oct 2026	Online	$1,100

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

Register Online Now

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