Cybersecurity in Health Data Research Training Course

Professional Development Training Course Outline

Category	Research and Data Analysis	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the digital age, health data has become an invaluable resource for research, policy-making, and improving patient outcomes. However, this sensitive information is increasingly vulnerable to cyber threats, breaches, and misuse. Cybersecurity in Health Data Research Training Course equips professionals with the necessary tools to safeguard data integrity, ensure compliance with privacy laws, and build resilient infrastructures. Through this course, participants will gain a practical understanding of cyber risk management, HIPAA compliance, data encryption, and incident response strategies specific to healthcare settings.

Designed for researchers, IT professionals, and healthcare administrators, this course bridges the knowledge gap between health informatics and cybersecurity best practices. Participants will engage in hands-on modules, case studies, and simulations to apply security strategies to real-world healthcare data research scenarios. This training is vital for professionals looking to enhance data protection, mitigate cyber threats, and maintain ethical standards in research involving electronic health records (EHRs), genomic data, and clinical trial data.

Programme Curriculum

Cybersecurity in Health Data Research Training Course

Introduction

In the digital age, health data has become an invaluable resource for research, policy-making, and improving patient outcomes. However, this sensitive information is increasingly vulnerable to cyber threats, breaches, and misuse. Cybersecurity in Health Data Research Training Course equips professionals with the necessary tools to safeguard data integrity, ensure compliance with privacy laws, and build resilient infrastructures. Through this course, participants will gain a practical understanding of cyber risk management, HIPAA compliance, data encryption, and incident response strategies specific to healthcare settings.

Designed for researchers, IT professionals, and healthcare administrators, this course bridges the knowledge gap between health informatics and cybersecurity best practices. Participants will engage in hands-on modules, case studies, and simulations to apply security strategies to real-world healthcare data research scenarios. This training is vital for professionals looking to enhance data protection, mitigate cyber threats, and maintain ethical standards in research involving electronic health records (EHRs), genomic data, and clinical trial data.

Course Objectives

By the end of this course, participants will be able to:

1. Understand the fundamentals of health data security and privacy principles.
2. Identify and assess cyber threats in health research environments.
3. Implement data protection techniques such as encryption and access control.
4. Apply HIPAA and GDPR regulations in health data management.
5. Develop and manage effective incident response plans.
6. Utilize cloud security protocols in healthcare research storage systems.
7. Analyze ethical concerns in digital health data usage.
8. Leverage blockchain for securing research data.
9. Integrate machine learning to detect and prevent cyber threats.
10. Secure medical IoT devices used in data collection.
11. Conduct risk assessments and penetration testing for health systems.
12. Understand the implications of AI in cybersecurity within health contexts.
13. Develop organizational cybersecurity policies and staff training programs.

Target Audiences

1. Health Data Researchers
2. Healthcare IT Professionals
3. Hospital and Clinic Administrators
4. Medical Informatics Specialists
5. Public Health Analysts
6. Data Governance Officers
7. Compliance and Legal Professionals
8. Cybersecurity Analysts in Healthcare

Course Duration: 10 days

Course Modules

Module 1: Introduction to Cybersecurity in Health Research

- Overview of cybersecurity principles
- Importance of cybersecurity in health research
- Major health data breaches: causes and impacts
- Cybersecurity frameworks (NIST, ISO)
- Ethics and data integrity
- **Case Study: Data breach in a university medical research center**

Module 2: Health Data Privacy and Legal Compliance

- HIPAA and GDPR essentials
- Patient consent and anonymization
- Cross-border data transfer rules
- Regulatory penalties and compliance
- Risk-based approaches to data handling

- **Case Study: GDPR compliance challenges in EU-funded research**

Module 3: Threat Landscape in Health Data Systems

- Malware, ransomware, phishing in healthcare
- Insider threats and accidental data exposure
- Social engineering and human factor risks
- Nation-state and cybercriminal group threats
- Threat intelligence platforms
- **Case Study: Ransomware attack on a hospital research lab**

Module 4: Encryption and Secure Communication

- Types of encryption (AES, RSA, TLS)
- End-to-end encryption in data exchange
- Public key infrastructure (PKI)
- Secure messaging tools for researchers
- Key management best practices
- **Case Study: Encryption failure and data leak incident**

Module 5: Access Control and Identity Management

- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Privilege escalation threats
- Identity and access management tools
- User behavior analytics
- **Case Study: Insider threat due to weak access policies**

Module 6: Secure Data Storage and Cloud Solutions

- Cloud providers for healthcare research
- Cloud encryption and segmentation
- Hybrid cloud models and risks
- Data integrity in distributed systems
- Business associate agreements (BAAs)
- **Case Study: Cloud misconfiguration in a genomic database**

Module 7: Risk Assessment and Vulnerability Testing

- Conducting cybersecurity risk assessments
- Penetration testing in health environments
- Vulnerability scanning tools
- Risk scoring models
- Gap analysis methods
- **Case Study: Red team exercise in clinical data center**

Module 8: Medical IoT and Connected Device Security

- IoT architecture in healthcare research
- Common vulnerabilities in medical devices
- Network segmentation for IoT
- Real-time monitoring solutions
- Device firmware management
- **Case Study: Exploitation of wearables in clinical trial**

Module 9: Incident Response and Recovery

- Incident response lifecycle
- Forensics in health data breaches
- Reporting obligations
- Disaster recovery planning
- Crisis communication strategies
- **Case Study: National health system response to data breach**

Module 10: Blockchain for Health Research Security

- Blockchain fundamentals
- Smart contracts in clinical trials
- Immutable audit trails
- Integration with existing databases
- Challenges in blockchain scalability
- **Case Study: Blockchain trial in a multi-center study**

Module 11: Artificial Intelligence for Cyber Defense

- AI vs traditional threat detection
- Machine learning for anomaly detection
- AI biases in health data security
- Automation of response actions
- Explainable AI in healthcare
- **Case Study: ML model prevents patient data leak**

Module 12: Ethical and Societal Dimensions

- Ethical principles in data handling
- Public trust and transparency
- Algorithmic accountability
- Health disparities and cybersecurity
- Digital inclusion
- **Case Study: Ethical dilemma in predictive analytics**

Module 13: Cybersecurity Workforce Training

- Cyber hygiene best practices
- Security awareness training programs
- Policy enforcement techniques
- Continuous education platforms
- Phishing simulation tools
- **Case Study: Impact of staff training on breach reduction**

Module 14: Emerging Technologies and Future Risks

- Quantum computing and data security
- 5G network implications
- Deepfakes and misinformation
- Augmented reality (AR) in clinical settings
- Emerging global cyber laws
- **Case Study: Predicting future risks in digital therapeutics**

Module 15: Capstone Project and Policy Development

- Cybersecurity policy writing
- Data governance frameworks

- Simulation of breach and response
- Peer reviews and presentations
- Final cybersecurity audit
- **Case Study: Group project on securing a digital health research hub**

Training Methodology

- Interactive instructor-led sessions
- Real-world case study discussions
- Hands-on labs and simulations
- Group breakout sessions and peer learning
- Final project with practical cybersecurity applications

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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