LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001H — Information Security Management for Health Data

ISO Certification Programme

LAPT — London Academy of Professional Training

Address 85 Great Portland Street, W1W 7LT, London, United Kingdom

Email info@lapt.org

Telephone +44 7513 283044

Web lapt.org

Reference HL-HIT-27001H • ISO Health

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	30	180	430	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**HL-HIT-27001H**
AWARD	**Certificate**
ASSESSMENT	**430 marks — 258 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Continuous Improvement Strategies

5 chapters · 30 classes · **45 marks**

- **1 Understanding Continuous Improvement in Health IT** — 6 classes
  - › 1.1 Define Key Concepts of Continuous Improvement in Health IT
  - › 1.2 Identify the Importance of Continuous Improvement for Health Data Security
  - › 1.3 Assess Current Continuous Improvement Practices in Health IT
  - › 1.4 Explore Tools and Techniques for Continuous Improvement in Health Services
  - › 1.5 Develop Actionable Improvement Plans Based on Analysis
  - › 1.6 Evaluate the Impact of Continuous Improvement Initiatives on Health IT Outcomes
- **2 Frameworks and Methodologies for Continuous Improvement** — 6 classes
  - › 2.1 Identify Key Continuous Improvement Frameworks in Information Security
  - › 2.2 Analyze the Role of Lean Methodology in Health Data Management
  - › 2.3 Explore Six Sigma Principles for Enhancing Data Security
  - › 2.4 Implement the PDCA Cycle for Continuous Improvement in Health Data Practices
  - › 2.5 Evaluate the Benefits of Agile Methodologies in Information Security Initiatives
  - › 2.6 Develop a Continuous Improvement Action Plan for Health Data Security
- **3 Measuring Performance and Outcomes in Health Data Security** — 6 classes
  - › 3.1 Define Key Performance Indicators for Health Data Security
  - › 3.2 Analyze Current Performance Metrics in Health Data Management
  - › 3.3 Implement Measurement Tools for Data Security Assessment
  - › 3.4 Evaluate Outcomes Based on Established Security Metrics
  - › 3.5 Identify Areas for Improvement in Health Data Security Practices
  - › 3.6 Develop an Action Plan for Continuous Improvement in Data Security
- **4 Engaging Stakeholders in Continuous Improvement Initiatives** — 6 classes
  - › 4.1 Identify Key Stakeholders for Improvement Initiatives
  - › 4.2 Analyze Stakeholder Needs and Expectations
  - › 4.3 Develop Effective Communication Strategies with Stakeholders
  - › 4.4 Foster Stakeholder Engagement through Collaborative Workshops
  - › 4.5 Measure Stakeholder Feedback and Satisfaction
  - › 4.6 Implement Stakeholder Recommendations for Continuous Improvement
- **5 Sustaining Continuous Improvement Over Time** — 6 classes
  - › 5.1 Assessing Current Continuous Improvement Practices in Health Data Management
  - › 5.2 Identifying Key Performance Indicators for Sustaining Improvements
  - › 5.3 Engaging Stakeholders in the Continuous Improvement Process
  - › 5.4 Implementing Feedback Mechanisms for Ongoing Improvement
  - › 5.5 Developing a Continuous Improvement Culture within Health Organizations
  - › 5.6 Evaluating Long-term Impact of Continuous Improvement Efforts

2 Data Privacy Regulations

5 chapters · 30 classes **65 marks**

• 1 Understanding Data Privacy Regulations in Health Care — 6 classes

- 1.1 Identify Key Data Privacy Regulations in Health Care
- 1.2 Explain the Importance of Data Privacy for Patient Trust
- 1.3 Analyze the Role of GDPR in Health Data Management
- 1.4 Distinguish Between Personal Data and Sensitive Data in Healthcare
- 1.5 Assess Compliance Requirements for Health Care Organizations
- 1.6 Develop Strategies for Implementing Data Privacy Practices

• 2 Overview of GDPR and its Implications for Health Data — 6 classes

- 2.1 Define GDPR: Explore Key Principles and Terminology
- 2.2 Identify Health Data: Understand What Constitutes Sensitive Data
- 2.3 Examine Rights of Individuals: Assess Key Rights Under GDPR
- 2.4 Analyze Responsibilities: Determine Obligations for Health Organizations
- 2.5 Evaluate GDPR Compliance: Review Strategies for Effective Implementation
- 2.6 Apply GDPR Principles: Develop Case Studies for Real-world Scenarios

• 3 Navigating UK Data Protection Laws Post-Brexit — 6 classes

- 3.1 Understand Key Changes in UK Data Protection Laws Post-Brexit
- 3.2 Identify the Impacts of GDPR on UK Data Practices
- 3.3 Explore the Role of the Information Commissioner's Office (ICO)
- 3.4 Assess Legal Bases for Processing Health Data in the UK
- 3.5 Implement Strategies for Compliance with UK Data Regulations
- 3.6 Evaluate the Importance of Data Subject Rights in Health Data Management

• 4 Risk Management Frameworks for Health Data Compliance — 6 classes

- 4.1 Identify Key Risk Factors in Health Data Compliance
- 4.2 Analyze Existing Risk Management Frameworks in Healthcare
- 4.3 Evaluate Risk Assessment Methodologies for Health Data
- 4.4 Develop Strategies for Mitigating Identified Risks
- 4.5 Integrate ISO 27001H Standards into Risk Management Practices
- 4.6 Implement Continuous Monitoring for Health Data Compliance Risks

• 5 Ethical Considerations and Best Practices in Health Data Privacy — 6 classes

- 5.1 Identify Ethical Dilemmas in Health Data Usage
- 5.2 Analyze the Impact of Data Privacy Regulations on Healthcare Practices
- 5.3 Explore Best Practices for Informed Consent in Health Data Collection
- 5.4 Evaluate Case Studies on Breaches of Health Data Privacy
- 5.5 Develop Policies for Ethical Management of Health Data
- 5.6 Implement Strategies for Continuous Improvement in Data Privacy Compliance

3 Information Security Principles

5 chapters · 30 classes **85 marks**

• 1 Fundamental Concepts of Information Security in Health Data — 6 classes

- 1.1 Define Key Terms in Information Security for Health Data
- 1.2 Identify Vulnerabilities in Health Data Management Systems
- 1.3 Analyze the Impact of Data Breaches in Healthcare
- 1.4 Assess the Importance of Confidentiality, Integrity, and Availability
- 1.5 Explore Best Practices for Protecting Health Data
- 1.6 Implement Basic Security Measures for Health Information Systems

• 2 Risk Management Strategies for Health Information Security — 6 classes

- 2.1 Identify key risks in health information security
- 2.2 Analyze the impact of data breaches in healthcare
- 2.3 Evaluate current risk management frameworks for health data
- 2.4 Develop mitigation strategies for identified risks
- 2.5 Implement risk assessment tools effectively
- 2.6 Monitor and review risk management practices in health information security

• 3 Legal and Ethical Considerations in Health Data Protection — 6 classes

- 3.1 Identify Key Legal Frameworks for Health Data Protection
- 3.2 Understand Ethical Principles in Handling Health Information
- 3.3 Analyze Case Studies on Legal Violations in Health Data
- 3.4 Evaluate the Role of Consent in Health Data Management
- 3.5 Explore Data Breach Notifications and Responsibilities
- 3.6 Develop a Compliance Checklist for Health Data Security

• 4 Implementing ISO 27001 Standards for Health IT — 6 classes

- 4.1 Understand ISO 27001 Standards and Their Importance in Health IT
- 4.2 Identify Key Components of an Information Security Management System (ISMS)
- 4.3 Assess Current Health IT Practices Against ISO 27001 Requirements
- 4.4 Develop an Effective Risk Assessment Strategy for Health Data
- 4.5 Implement Data Protection Policies Aligned with ISO 27001 Standards
- 4.6 Evaluate and Review ISO 27001 Implementation Outcomes in Health IT

• 5 Continuous Improvement and Compliance Monitoring in Health Data Security — 6 classes

- 5.1 Identify Key Metrics for Health Data Security Improvement
- 5.2 Analyze Current Compliance Status Against ISO 27001 Standards
- 5.3 Develop Action Plans for Addressing Compliance Gaps
- 5.4 Implement Continuous Monitoring Tools for Health Data Security
- 5.5 Conduct Regular Reviews and Audits of Security Measures
- 5.6 Foster a Culture of Security Awareness and Continuous Improvement

4 ISO 27001 Implementation

5 chapters · 30 classes **85 marks**

- **1 Understanding ISO 27001 Fundamentals for Health Data** — 6 classes
  - 1.1 Define ISO 27001 and its relevance to health data management
  - 1.2 Identify key components of the ISO 27001 standard
  - 1.3 Explore the importance of risk assessment in ISO 27001
  - 1.4 Understand the role of leadership in ISO 27001 implementation
  - 1.5 Analyze the steps for developing an Information Security Management System (ISMS)
  - 1.6 Apply ISO 27001 principles to create an action plan for health data security
- **2 Scope and Context in ISO 27001 for Health IT** — 6 classes
  - 2.1 Define the Scope of ISO 27001 in Health IT
  - 2.2 Analyze the Context of Health Data Security
  - 2.3 Identify Stakeholders Involved in Health IT Security
  - 2.4 Assess Internal and External Factors Affecting Compliance
  - 2.5 Develop Objectives Based on Context and Scope
  - 2.6 Create a Roadmap for Implementing ISO 27001 Framework
- **3 Risk Assessment and Treatment in Health Data Security** — 6 classes
  - 3.1 Identify Key Risks in Health Data Security
  - 3.2 Assess Vulnerabilities in Health Information Systems
  - 3.3 Evaluate Potential Impact of Health Data Breaches
  - 3.4 Develop Risk Mitigation Strategies for Health Data
  - 3.5 Implement Risk Treatment Plans in Healthcare Settings
  - 3.6 Monitor and Review Risk Management Practices in Health Data Security
- **4 Implementing ISO 27001 Controls for Health Organizations** — 6 classes
  - 4.1 Identify Key ISO 27001 Controls for Health Data Protection
  - 4.2 Assess Current Health Organization Security Practices
  - 4.3 Develop a Risk Management Framework for Health Data
  - 4.4 Implement Access Control Measures for Sensitive Health Information
  - 4.5 Monitor and Review ISO 27001 Compliance in Health Organizations
  - 4.6 Create an Action Plan for Continuous Improvement in Information Security
- **5 Continuous Improvement and Audit for ISO 27001 Compliance** — 6 classes
  - 5.1 Assess Current Compliance Levels Using ISO 27001 Standards
  - 5.2 Identify Key Performance Indicators for Continuous Improvement
  - 5.3 Develop an Audit Plan Focused on Health Data Security
  - 5.4 Execute Internal Audits and Gather Findings for ISO 27001
  - 5.5 Create Action Plans for Addressing Audit Findings and Enhancing Compliance
  - 5.6 Establish a Culture of Continuous Improvement in Information Security Management

5 Leadership in Information Security

5 chapters · 30 classes **85 marks**

- **1 Understanding Leadership Roles in Information Security for Health Data** — 6 classes
  - 1.1 Define Key Leadership Concepts in Information Security
  - 1.2 Identify the Roles and Responsibilities of Information Security Leaders
  - 1.3 Analyze the Importance of Leadership in Health Data Security
  - 1.4 Explore Case Studies of Effective Leadership in Information Security
  - 1.5 Evaluate Challenges Faced by Leaders in Protecting Health Data
  - 1.6 Develop an Action Plan for Enhancing Leadership in Information Security
- **2 Frameworks and Standards: Implementing ISO 27001 in Health IT** — 6 classes
  - 2.1 Understand the Importance of ISO 27001 in Health IT
  - 2.2 Identify Key Components of the ISO 27001 Framework
  - 2.3 Analyze Current Health IT Practices Against ISO 27001 Standards
  - 2.4 Develop a Gap Analysis for ISO 27001 Implementation
  - 2.5 Create an Implementation Plan for ISO 27001 in Health Organisations
  - 2.6 Evaluate Success Metrics for ISO 27001 Compliance in Health IT
- **3 Risk Management Strategies for Protecting Health Information** — 6 classes
  - 3.1 Identify Key Risks to Health Information Security
  - 3.2 Assess Impact of Risks on Health Data
  - 3.3 Determine Likelihood of Risk Occurrence
  - 3.4 Develop Mitigation Strategies for Identified Risks
  - 3.5 Implement Risk Management Framework in Health Organizations
  - 3.6 Evaluate Effectiveness of Risk Management Strategies in Practice
- **4 Building a Culture of Security: Engagement and Training** — 6 classes
  - 4.1 Assessing Current Security Culture in Health Organizations
  - 4.2 Identifying Key Stakeholders for Security Engagement
  - 4.3 Designing Effective Training Programs for Health Data Security
  - 4.4 Implementing Continuous Learning and Security Awareness Initiatives
  - 4.5 Measuring Engagement and Training Impact on Security Culture
  - 4.6 Developing Action Plans for Sustained Security Culture Improvement
- **5 Measuring Success: Metrics and Continuous Improvement in Information Security** — 6 classes
  - 5.1 Define Key Performance Indicators for Information Security Success
  - 5.2 Analyze Current Metrics in Information Security Practices
  - 5.3 Implement Metrics Tracking Tools for Health Data Security
  - 5.4 Evaluate the Effectiveness of Information Security Metrics
  - 5.5 Develop a Continuous Improvement Plan for Security Metrics
  - 5.6 Communicate Metrics Findings to Stakeholders for Enhanced Leadership

6 Risk Management in Health IT

5 chapters · 30 classes **65 marks**

• 1 Understanding Risk Management Principles in Health IT — 6 classes

- 1.1 Define Risk Management Principles in Health IT
- 1.2 Identify Common Risks in Health IT Environments
- 1.3 Analyze the Impact of Risks on Health Data Security
- 1.4 Implement Risk Assessment Methodologies in Health IT
- 1.5 Evaluate Risk Mitigation Strategies for Health Systems
- 1.6 Develop a Risk Management Framework for Health IT

• 2 Identifying Risks in Health IT Environments — 6 classes

- 2.1 Understand Basic Risks in Health IT Environments
- 2.2 Identify Common Threats to Health Data Security
- 2.3 Assess Vulnerabilities in Health IT Systems
- 2.4 Analyze the Impact of Risks on Health Care Services
- 2.5 Evaluate Risk Levels Using a Risk Matrix
- 2.6 Develop a Risk Identification Plan for Health IT Projects

• 3 Assessing and Analyzing Risks in Health IT — 6 classes

- 3.1 Identify Key Risks in Health IT Systems
- 3.2 Evaluate the Impact of Risks on Patient Safety
- 3.3 Analyze Vulnerabilities in Health Data Management
- 3.4 Prioritize Risks Using a Risk Matrix
- 3.5 Develop Mitigation Strategies for Identified Risks
- 3.6 Implement Continuous Risk Monitoring Practices

• 4 Implementing Risk Mitigation Strategies in Health Data Management — 6 classes

- 4.1 Identify Key Risks in Health Data Management
- 4.2 Assess Impact and Likelihood of Identified Risks
- 4.3 Develop Prioritized Risk Mitigation Strategies
- 4.4 Implement Risk Mitigation Strategies in Practice
- 4.5 Monitor and Review Risk Mitigation Effectiveness
- 4.6 Communicate Risk Management Outcomes to Stakeholders

• 5 Monitoring and Reviewing Risk Management Frameworks in Health IT — 6 classes

- 5.1 Identify Key Risk Indicators in Health IT
- 5.2 Analyze Current Risk Management Frameworks for Effectiveness
- 5.3 Evaluate the Impact of Changes in Health IT on Risk Management
- 5.4 Develop a Monitoring Plan for Health IT Risks
- 5.5 Implement Continuous Improvement Strategies in Risk Management
- 5.6 Present Findings from Risk Management Reviews to Stakeholders