LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 27001 — Information Security for Patient Data Protection

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

CURRICULUM

1 Data Protection Regulations

5 chapters · 30 classes · **65 marks**

- **1 Introduction to Data Protection Regulations** — 6 classes
  - 1.1 Define Key Concepts in Data Protection Regulations
  - 1.2 Explore the Significance of Patient Data Protection
  - 1.3 Identify Key Legislation Affecting Healthcare Data
  - 1.4 Analyze the Role of ISO 27001 in Data Protection
  - 1.5 Examine Compliance Requirements for Healthcare Organizations
  - 1.6 Develop a Basic Action Plan for Implementing Data Protection Strategies
- **2 Understanding GDPR and Its Impact on Patient Data** — 6 classes
  - 2.1 Define GDPR and its Key Principles
  - 2.2 Identify the Rights of Patients Under GDPR
  - 2.3 Explore the Responsibilities of Healthcare Providers
  - 2.4 Analyze the Consequences of GDPR Non-Compliance
  - 2.5 Examine Case Studies of GDPR in Healthcare
  - 2.6 Implement Strategies for GDPR Compliance in Patient Data Management
- **3 Roles and Responsibilities in Data Protection** — 6 classes
  - 3.1 Identify Key Roles in Data Protection Management
  - 3.2 Describe Responsibilities of Data Controllers
  - 3.3 Explain the Role of Data Processors in Patient Data Handling
  - 3.4 Outline Accountability Measures in Data Protection Leadership
  - 3.5 Assess Compliance Requirements for Different Roles
  - 3.6 Develop an Action Plan for Role-specific Data Protection Training
- **4 Risk Assessment and Management for Patient Data** — 6 classes
  - 4.1 Identify Key Components of Risk Assessment for Patient Data
  - 4.2 Analyze Potential Risks to Patient Data Security
  - 4.3 Evaluate Impact and Likelihood of Identified Risks
  - 4.4 Develop Mitigation Strategies for Patient Data Risks
  - 4.5 Implement Risk Management Plans for Patient Data Protection
  - 4.6 Monitor and Review Risk Management Effectiveness for Patient Data
- **5 Continuous Improvement and Compliance Monitoring** — 6 classes
  - 5.1 Evaluate Current Compliance Practices for Patient Data
  - 5.2 Identify Key Performance Indicators for Continuous Improvement
  - 5.3 Implement Regular Audits to Monitor Data Protection Compliance
  - 5.4 Analyze Audit Results to Identify Areas for Improvement
  - 5.5 Develop Action Plans Based on Audit Findings and Compliance Gaps
  - 5.6 Foster a Culture of Continuous Improvement in Data Protection

2 Implementation Strategies

5 chapters · 30 classes **85 marks**

- **1 Understanding ISO 27001 Framework and Its Relevance to Patient Data Protection** — 6 classes
  - 1.1 Explore the Key Components of the ISO 27001 Framework
  - 1.2 Analyze the Importance of ISO 27001 for Patient Data Protection
  - 1.3 Identify Roles and Responsibilities in Implementing ISO 27001
  - 1.4 Evaluate Risk Assessment Techniques within the ISO 27001 Context
  - 1.5 Develop an Action Plan for ISO 27001 Compliance in Healthcare
  - 1.6 Review Case Studies of ISO 27001 Implementation in Patient Data Security
- **2 Risk Assessment and Management for Patient Data: Identifying Vulnerabilities** — 6 classes
  - 2.1 Define Key Concepts in Risk Assessment for Patient Data
  - 2.2 Identify Common Vulnerabilities in Patient Data Management
  - 2.3 Analyze Potential Threats to Patient Data Security
  - 2.4 Assess the Impact of Vulnerabilities on Patient Care
  - 2.5 Develop a Risk Assessment Framework for Patient Data
  - 2.6 Create an Action Plan for Mitigating Identified Risks
- **3 Designing and Implementing an Information Security Management System (ISMS) for Healthcare** — 6 classes
  - 3.1 Assess Current Information Security Frameworks in Healthcare
  - 3.2 Identify Key Regulations and Standards for Patient Data
  - 3.3 Develop a Risk Assessment Plan for Healthcare Data Security
  - 3.4 Design Security Policies and Procedures for Patient Data Protection
  - 3.5 Implement Training and Awareness Programs for Healthcare Staff
  - 3.6 Evaluate and Monitor the Effectiveness of the ISMS Implementation
- **4 Developing Policies and Procedures for Compliance with ISO 27001** — 6 classes
  - 4.1 Identify Key Components of ISO 27001 Policies
  - 4.2 Analyze Patient Data Protection Requirements
  - 4.3 Develop Comprehensive Procedures for Risk Assessment
  - 4.4 Create Incident Response Policies for Data Breaches
  - 4.5 Establish Monitoring and Review Mechanisms for Compliance
  - 4.6 Implement Training Strategies for Policy Awareness
- **5 Monitoring, Reviewing, and Continual Improvement of Information Security Strategies** — 6 classes
  - 5.1 Assess Current Information Security Strategies through Monitoring Techniques
  - 5.2 Review Data Protection Policies for Compliance and Effectiveness
  - 5.3 Identify Key Performance Indicators for Information Security Management
  - 5.4 Conduct Gap Analysis to Determine Areas for Improvement
  - 5.5 Implement Recommendations for Enhanced Data Protection Strategies
  - 5.6 Establish a Framework for Ongoing Review and Continual Improvement

3 Information Security Management Systems

5 chapters · 30 classes **85 marks**

- **1 Fundamentals of Information Security Management Systems in Healthcare** — 6 classes
  - 1.1 Define Key Concepts in Information Security Management Systems
  - 1.2 Identify Regulatory Requirements for Patient Data Protection
  - 1.3 Assess Risks Associated with Healthcare Information Security
  - 1.4 Implement Core Principles of Information Security in Healthcare
  - 1.5 Develop an Information Security Policy for Healthcare Settings
  - 1.6 Evaluate the Effectiveness of Information Security Practices in Healthcare
- **2 Understanding ISO 27001 Standards and Frameworks** — 6 classes
  - 2.1 Explore the Key Principles of ISO 27001 for Patient Data Protection
  - 2.2 Identify the Components of an Information Security Management System (ISMS)
  - 2.3 Assess the Role of Risk Management in ISO 27001 Compliance
  - 2.4 Analyze the Benefits of Implementing ISO 27001 in Healthcare Settings
  - 2.5 Examine the Steps to Achieving ISO 27001 Certification
  - 2.6 Apply ISO 27001 Standards to Develop a Patient Data Protection Plan
- **3 Risk Assessment and Management in Patient Data Security** — 6 classes
  - 3.1 Identify Key Risks in Patient Data Security
  - 3.2 Analyze Vulnerabilities in Information Security Systems
  - 3.3 Evaluate the Impact of Data Breaches on Patient Privacy
  - 3.4 Develop a Risk Assessment Framework for Patient Data
  - 3.5 Implement Risk Mitigation Strategies in Healthcare Settings
  - 3.6 Review and Update the Risk Management Plan Regularly
- **4 Implementing Security Controls and Best Practices** — 6 classes
  - 4.1 Identify Key Security Controls for Patient Data Protection
  - 4.2 Assess Risks Associated with Patient Data Handling
  - 4.3 Develop a Framework for Security Best Practices
  - 4.4 Implement Technical Security Controls Across Systems
  - 4.5 Establish Policies for Staff Training and Awareness
  - 4.6 Monitor and Review Security Controls for Continuous Improvement
- **5 Continuous Improvement and Compliance Monitoring in ISMS** — 6 classes
  - 5.1 Understand the Concept of Continuous Improvement in ISMS
  - 5.2 Explore Key Principles of Compliance Monitoring
  - 5.3 Analyze the Role of Leadership in Promoting Continuous Improvement
  - 5.4 Identify Metrics for Measuring ISMS Effectiveness
  - 5.5 Implement a Plan for Regular Compliance Audits
  - 5.6 Develop Strategies for Addressing Non-Compliance Findings

4 Leadership in Information Security

5 chapters · 30 classes **45 marks**

• 1 Understanding ISO 27001 and Its Importance in Health Care Services — 6 classes

- 1.1 Define ISO 27001 and Its Relevance to Healthcare
- 1.2 Explore the Key Principles of Information Security
- 1.3 Identify the Benefits of ISO 27001 for Patient Data Protection
- 1.4 Analyze Case Studies of ISO 27001 Implementation in Healthcare
- 1.5 Develop an Action Plan for ISO 27001 Compliance in Your Organization
- 1.6 Evaluate the Role of Leadership in Upholding ISO 27001 Standards

• 2 Roles and Responsibilities in Information Security Leadership — 6 classes

- 2.1 Define Key Leadership Roles in Information Security
- 2.2 Identify Responsibilities of Information Security Leaders
- 2.3 Analyze the Impact of Leadership on Security Culture
- 2.4 Develop Skills Essential for Information Security Leadership
- 2.5 Create a Framework for Delegating Security Responsibilities
- 2.6 Assess Leadership Strategies for Engaging Stakeholders in Security

• 3 Risk Management Framework in Health Care Information Security — 6 classes

- 3.1 Identify Key Components of the Risk Management Framework
- 3.2 Assess Risks to Patient Data in a Healthcare Environment
- 3.3 Implement Risk Mitigation Strategies for Patient Data Protection
- 3.4 Evaluate the Effectiveness of Risk Management Practices
- 3.5 Communicate Risk Management Plans to Stakeholders
- 3.6 Integrate Continuous Improvement into Risk Management Processes

• 4 Developing and Implementing an Information Security Policy — 6 classes

- 4.1 Define Key Components of an Information Security Policy
- 4.2 Identify Stakeholders in Policy Development
- 4.3 Assess Risks and Compliance Requirements for Patient Data
- 4.4 Draft Initial Policy Framework for Information Security
- 4.5 Engage Stakeholders for Feedback and Consensus
- 4.6 Implement and Communicate the Finalized Information Security Policy

• 5 Continuous Improvement and Leadership in Information Security — — 6 classes

- 5.1 Identify Key Principles of Continuous Improvement in Information Security
- 5.2 Analyze Challenges in Implementing ISO 27001 Standards
- 5.3 Develop Strategies for Enhancing Patient Data Protection
- 5.4 Foster a Culture of Security Awareness Among Healthcare Staff
- 5.5 Create a Framework for Measuring Information Security Performance
- 5.6 Implement Actionable Feedback Loops for Ongoing Security Enhancement

5 Monitoring and Review

5 chapters · 30 classes **65 marks**

• 1 Understanding Monitoring Principles in Information Security — 6 classes

- 1.1 Define Key Monitoring Principles in Information Security
- 1.2 Identify Regulatory Requirements for Patient Data Monitoring
- 1.3 Analyze Techniques for Effective Data Monitoring
- 1.4 Evaluate Monitoring Tools for Patient Data Security
- 1.5 Develop a Monitoring Strategy for ISO 27001 Compliance
- 1.6 Implement Continuous Monitoring Practices in Healthcare Settings

• 2 Regulatory Compliance and Best Practices for Patient Data — 6 classes

- 2.1 Identify Key Regulations Affecting Patient Data Management
- 2.2 Analyze Best Practices for Compliance with ISO 27001
- 2.3 Conduct a Gap Analysis for Current Data Protection Practices
- 2.4 Develop a Monitoring Framework for Ongoing Compliance
- 2.5 Evaluate the Effectiveness of Existing Patient Data Security Measures
- 2.6 Create an Action Plan for Continuous Improvement in Data Protection

• 3 Developing Effective Monitoring Strategies for Health Services — 6 classes

- 3.1 Identify Key Indicators for Patient Data Security
- 3.2 Establish Baseline Metrics for Monitoring Compliance
- 3.3 Develop a Risk Assessment Framework for Health Services
- 3.4 Create Data Collection Methods for Ongoing Monitoring
- 3.5 Analyze Monitoring Data to Identify Trends and Issues
- 3.6 Implement Continuous Improvement Strategies for Data Protection

• 4 Leveraging Technology for Enhanced Monitoring of Patient Data — 6 classes

- 4.1 Analyze Current Monitoring Tools for Patient Data
- 4.2 Evaluate the Role of Automation in Data Monitoring
- 4.3 Implement Real-Time Data Tracking Solutions
- 4.4 Integrate Advanced Analytics for Enhanced Insights
- 4.5 Compare Cloud vs On-Premises Solutions for Data Security
- 4.6 Develop a Continuous Improvement Plan for Monitoring Systems

• 5 Evaluating and Reviewing Monitoring Effectiveness — 6 classes

- 5.1 Assess Current Monitoring Practices for Patient Data
- 5.2 Identify Key Performance Indicators for Monitoring Effectiveness
- 5.3 Analyze Data Collection Methods for Security Monitoring
- 5.4 Evaluate Risk Assessment Procedures in Monitoring
- 5.5 Recommend Improvements Based on Monitoring Evaluations
- 5.6 Develop an Action Plan for Ongoing Review and Adaptation

6 Risk Assessment and Management

5 chapters · 30 classes **85 marks**

• 1 Understanding Risk Assessment Concepts in Healthcare — 6 classes

- 1.1 Define Key Risk Assessment Terminology in Healthcare
- 1.2 Identify Common Risks to Patient Data Security
- 1.3 Analyze the Importance of Risk Assessment in Healthcare Settings
- 1.4 Evaluate Risk Assessment Methodologies Applied to Patient Data
- 1.5 Develop a Basic Risk Assessment Framework for Healthcare
- 1.6 Implement Risk Mitigation Strategies for Patient Data Protection

• 2 Identifying and Analyzing Risks in Patient Data Management — 6 classes

- 2.1 Define Key Concepts in Patient Data Risk Management
- 2.2 Identify Common Risks Associated with Patient Data Handling
- 2.3 Analyze the Impact of Identified Risks on Patient Safety
- 2.4 Evaluate Existing Controls for Mitigating Risks in Patient Data
- 2.5 Develop a Risk Assessment Matrix for Patient Data Scenarios
- 2.6 Create an Action Plan for Risk Mitigation in Patient Data Management

• 3 Implementing ISO 27001 Standards for Risk Management — 6 classes

- 3.1 Identify Key Components of ISO 27001 for Risk Management
- 3.2 Assess Current Risk Management Practices in Healthcare
- 3.3 Conduct a Gap Analysis for ISO 27001 Compliance
- 3.4 Develop Risk Assessment Methodologies for Patient Data
- 3.5 Create a Risk Treatment Plan Aligned with ISO 27001 Standards
- 3.6 Implement Continuous Monitoring and Improvement for Risk Management

• 4 Conducting Effective Risk Assessments in Clinical Environments — 6 classes

- 4.1 Identify Critical Assets in Clinical Environments
- 4.2 Evaluate Threats to Patient Data in Healthcare Settings
- 4.3 Analyze Vulnerabilities in Clinical Information Systems
- 4.4 Assess Risks Using a Quantitative Risk Assessment Method
- 4.5 Develop Risk Mitigation Strategies for Patient Data Protection
- 4.6 Implement and Monitor Risk Management Plans in Clinical Practice

• 5 Continuously Monitoring and Reviewing Risk Management Strategies — 6 classes

- 5.1 Define Continuous Monitoring in Risk Management
- 5.2 Identify Key Indicators for Effective Risk Assessment
- 5.3 Evaluate Current Risk Management Strategies
- 5.4 Implement Tools for Continuous Risk Monitoring
- 5.5 Review and Update Risk Management Policies Regularly
- 5.6 Communicate Findings and Adjust Strategies Accordingly