



Advanced Medical Confidentiality and Patient Information Governance Training Course

22 – 26 February 2027
Kuala Lumpur

Advanced Medical Confidentiality and Patient Information Governance Training Course

Ref: 1508_211344 **Date:** 22 – 26 February 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Advanced Medical Confidentiality and Patient Information Governance Training Course is a one-week course for healthcare managers, clinical governance leaders, information professionals, and privacy functions, who leave with a Patient Information Governance Assurance File. The course connects ethical duties, lawful use and disclosure, consent, access rights, minimum-necessary controls, digital communication, incident response, and accountability. Agile Leaders Training Center presents medical confidentiality as a patient-information governance discipline.

Who Should Attend

- Functions responsible for clinical governance and patient trust
- Teams responsible for health records and information access
- Personnel responsible for privacy, compliance, and disclosure decisions
- Leaders responsible for digital health communication and data sharing
- Departments responsible for confidentiality incidents and corrective action

The course assumes participants influence patient-information decisions at work and leaves out jurisdiction-specific legal advice and technical cybersecurity engineering.

Departments and Industries

The course supports departments handling sensitive health information across care delivery, insurance, research, and digital health services.

- Hospitals, clinics, and diagnostic services
- Health information and medical records functions
- Clinical governance and quality departments
- Health insurance and claims operations
- Research institutions and digital health providers

Learning Objectives

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



- Analyze ethical and lawful bases for handling patient information
- Apply minimum-necessary and purpose-limitation controls
- Evaluate consent, access, and disclosure requests
- Build confidentiality controls for records and digital communication
- Diagnose breaches and prioritize response actions
- Use governance evidence to assure accountability

Course Agenda

Day 1: Confidentiality Duties and Decisions

- Patient Trust and Ethical Duty Decision Map
- Personal and Health Information Classification Matrix
- Purpose Limitation and Minimum-Necessary Test
- Confidentiality Responsibility and Accountability Charter
- Applicable-Law and Professional-Duty Register

Day 2: Consent, Access, and Disclosure

- Consent Validity and Scope Assessment
- Patient Access and Representative Request Workflow
- Direct-Care Information Sharing Decision Tree
- Non-Care Disclosure Justification Record
- Public-Interest and Mandatory Disclosure Escalation Path

Day 3: Operational Information Controls

- Role-Based Patient Information Access Matrix
- Records Handling and Secure Disposal Checklist
- Digital Messaging and Remote Communication Control Standard
- Third-Party Processing and Data-Sharing Control Schedule
- Confidentiality Training and Sanctions Framework

Day 4: Breach Response and Assurance

- Confidentiality Incident Triage Method
- Health-Data Breach Impact Assessment
- Containment, Mitigation, and Notification Playbook
- Disclosure and Incident Evidence Register
- Privacy Control Audit and Improvement Cycle



Day 5: Patient Information Governance Practice

- Suggested Exercise: Consent and Disclosure Decision
- Suggested Exercise: Minimum-Necessary Access Review
- Suggested Exercise: Digital Communication Risk Control
- Suggested Exercise: Confidentiality Breach Escalation
- Capstone Exercise: Patient Information Governance Assurance File

Practical Exercises

The course uses suggested activities based on fictional care, insurance, research, and digital health scenarios.

- Suggested activity: classify patient information and document a justified use or disclosure decision.
- Suggested activity: evaluate access, consent, representative, and public-interest requests using a decision record.
- Suggested activity: triage a messaging-related confidentiality incident and select containment, mitigation, and escalation actions.
- Suggested activity: present an assurance file linking controls, evidence, ownership, and improvement actions.

FAQs

Who suits advanced medical confidentiality training, and what does it assume?

Healthcare governance, records, privacy, compliance, and departmental leaders suit the training; it assumes responsibility for patient-information decisions and organizational controls.

How does patient information governance differ from general data protection training?

Patient information governance applies privacy principles to clinical trust, care sharing, medical records, consent, disclosure, access, digital communication, and health-data incidents rather than treating personal data only as a general compliance topic.

When may confidential patient information be disclosed?

Patient information may be disclosed when a valid consent, direct-care need, legal requirement, or defensible public-interest basis applies, with the scope limited, the recipient verified, and the decision documented.

What does minimum necessary mean for medical confidentiality?

Minimum necessary means limiting access, use, or disclosure to the people, information, and purpose needed for the authorized task while preserving appropriate information sharing for safe care.



How should a medical confidentiality breach be managed?

A confidentiality breach should be identified, contained, assessed, documented, escalated, mitigated, and notified under the applicable organizational and legal requirements, followed by corrective action and control review.

Conclusion

Participants leave with a Patient Information Governance Assurance File containing decision, access, disclosure, communication, incident, and audit tools. The file creates a traceable route from an information request or event to an accountable response. It helps organizations protect confidentiality while supporting lawful information use and safe care.