



Healthcare Data Protection and Patient Confidentiality Training Course

26 – 30 April 2027
Milan



AGILE LEADERS
Training Center

Healthcare Data Protection and Patient Confidentiality Training Course

Ref: 820_162124 **Date:** 26 – 30 April 2027 **Location:** Milan **Fees:** 5700 Euro

Overview

Healthcare Data Protection and Patient Confidentiality Training Course is a five-day intermediate course for healthcare operations, health information, privacy, compliance, digital health, and service-partner functions who leave with a Healthcare Privacy and Confidentiality Pack. Participants map patient-data journeys, classify sensitive information, define confidentiality and access rules, control sharing and vendors, manage rights and retention, coordinate incidents, and test evidence across clinical and administrative scenarios. Agile Leaders Training Center develops practical healthcare information protection capability.

Who Should Attend

- Healthcare operations functions responsible for patient journeys, appointments, treatment support, and administration
- Health information functions responsible for medical records, coding, release, retention, and data quality
- Privacy and compliance functions responsible for requirements, rights, incidents, and assurance
- Digital health and technology governance functions responsible for systems, portals, integrations, and access
- Clinical governance functions responsible for confidentiality decisions and appropriate information sharing
- Procurement and vendor functions responsible for processors, service partners, and data exchanges

The course assumes participants already handle healthcare information or control related processes, and leaves out clinical decision-making, legal representation, penetration testing, and certification examination preparation.

Departments and Industries

The course supports departments and industries that create, use, share, store, or protect patient and workforce health information.

- Clinical operations, patient services, medical records, coding, billing, and quality
- Privacy, compliance, risk, audit, legal operations, and information governance
- Digital health, information technology, cybersecurity coordination, procurement, and vendors
- Hospitals, clinics, laboratories, pharmacies, insurers, and telehealth services
- Research organizations, rehabilitation providers, care networks, and health-service suppliers

Learning Objectives

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

- Map healthcare data flows and assign accountable owners
- Apply confidentiality and lawful-handling decisions
- Build role-based access, sharing, and retention controls
- Manage patient rights and healthcare vendor obligations
- Analyze privacy risks and coordinate data incidents
- Build a Healthcare Privacy and Confidentiality Pack

Course Agenda

Day 1: Map Patient Data and Confidentiality Duties

- Patient and Workforce Information Inventory
- Clinical and Administrative Data Flow Map
- Health Information Classification Guide
- Confidentiality Responsibility Matrix
- Healthcare Privacy Risk Register

Day 2: Control Access and Information Use

- Role-Based Access Decision Table
- Medical Record Viewing and Update Rules
- Identity Verification and Disclosure Check
- Minimum-Necessary Information Review
- Access Logging and Exception Monitoring

Day 3: Govern Sharing, Digital Health, and Vendors

- Care Coordination and Referral Sharing Checklist
- Patient Portal and Digital Health Privacy Review
- Vendor and Service-Partner Due Diligence
- Data-Sharing Agreement Control Matrix
- Secondary Use and Research Decision Record

Day 4: Manage Rights, Retention, and Incidents

- Patient Information Rights Workflow
- Correction, Restriction, and Release Log
- Health Record Retention and Disposal Schedule
- Healthcare Data Incident Triage Matrix
- Breach Escalation and Communication Record



Day 5: Test Healthcare Privacy and Confidentiality

- Control Evidence and Assurance Checklist
- Privacy Metrics and Exception Dashboard
- Exercise: Resolve a Confidentiality Decision
- Exercise: Coordinate a Patient Data Incident
- Capstone: Healthcare Privacy and Confidentiality Pack

Practical Exercises

The course uses suggested activities based on appointments, medical records, referrals, patient portals, billing, research, vendors, and workforce scenarios.

- Suggested activity: trace a patient-data journey and record owners, access points, sharing events, and risks.
- Suggested activity: evaluate a disclosure request and apply identity, authority, purpose, and minimum-necessary checks.
- Suggested activity: review a digital-health vendor and define access, sharing, retention, incident, and assurance controls.
- Suggested activity: triage a patient-data incident, coordinate decisions, and assemble closure evidence.

FAQs

Who suits healthcare data protection training, and what does it assume?

Healthcare operations, records, privacy, compliance, digital health, clinical governance, procurement, and vendor functions suit the training; it assumes practical familiarity with patient or workforce information processes.

How does patient confidentiality differ from data protection?

Patient confidentiality governs trusted use and disclosure of information obtained through care, while data protection applies broader principles, rights, responsibilities, safeguards, and accountability across the information lifecycle. Operational controls should support both.

What should a healthcare data flow map contain?

The map should record information categories, patients and staff, collection points, care and administrative purposes, systems, users, disclosures, vendors, storage, retention, disposal, safeguards, and accountable owners.



How should healthcare organizations control information sharing?

Organizations should verify identity and authority, define the purpose and permitted scope, limit information, use approved channels, record disclosures, control onward sharing, honor applicable rights and restrictions, and monitor exceptions.

What evidence supports healthcare privacy assurance?

Evidence includes inventories, flow maps, access decisions, disclosure logs, rights records, retention schedules, vendor reviews, agreements, risk assessments, incident records, training, control tests, exceptions, remediation, and management review.

Conclusion

Participants take back a Healthcare Privacy and Confidentiality Pack containing data inventories, flow maps, classification and access rules, disclosure checks, sharing controls, vendor reviews, rights workflows, retention schedules, incident records, and assurance measures. It connects patient confidentiality with repeatable controls across clinical, administrative, and digital services. The pack provides a practical structure for decisions, evidence, escalation, and improvement.