JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Patient Confidentiality and Health Records Privacy Training Course

3 – 7 January 2027
Kuala Lumpur

Patient Confidentiality and Health Records Privacy Training Course

Ref: 3124_126261 **Date:** 3 – 7 January 2027 **Location:** Kuala Lumpur **Fees:** 4600 GBP

Patient Confidentiality and Health Records Privacy is a 1-week training course for health records, clinical governance and patient services staff, in which each participant builds a patient confidentiality control plan for one department. Electronic records now follow patients across clinics, laboratories, pharmacies and insurers, so a careless disclosure travels further than a lost paper chart. Jupiter Prime Training offers this course on patient confidentiality and health records privacy.

Why Patient Confidentiality and Health Records Privacy Matters Now

Three pressures shape this field today. Shared clinical systems let many professionals open a single chart. Patients ask more often to see, correct or restrict their records. Insurers and researchers request extracts that need case-by-case justification. Guarding records well keeps patient trust; failing brings complaints and sanctions under the applicable health information rules.

Who Gains Most from Patient Confidentiality and Health Records Privacy

- Those who file, retrieve, release and archive medical records and answer requests for copies
- Those who oversee clinical governance, audit chart access and investigate confidentiality concerns
- Those who run patient services desks, registration, appointment lines and complaints
- Those who administer clinical system accounts, roles and audit trails
- Those who coordinate referrals, insurer claims and research extracts that leave the department

A hospital department or clinic network gains most when its records lead, governance officer and patient services supervisor attend side by side.

Patient Confidentiality and Health Records Privacy Capabilities

Participants judge each disclosure against its clinical purpose and set chart controls.

- Assess whether a request to share a record has a lawful and clinical justification — release of information officers
- Design role-based access to clinical systems by ward, specialty and shift — system administrators
- Apply minimum-necessary disclosure to referrals, claims and research extracts — governance committees
- Build a routine for patient access, correction and restriction requests — patient services leads
- Test audit trails for inappropriate chart viewing — clinical governance officers
-

Communicate a confidentiality breach response to patients and leadership — the department head

Key Patient Confidentiality and Health Records Privacy Terms

- Duty of confidence — the professional and legal obligation of clinicians and staff to keep what patients disclose private.
- Implied consent for care — the accepted assumption that patients agree to sharing among the professionals directly treating them.
- Minimum necessary — releasing only the part of a record that a stated purpose actually requires.
- Break-the-glass access — emergency override that opens a restricted chart and records who opened it and why.
- Pseudonymisation — replacing patient identifiers with codes so records can be studied without naming the individual.
- Access audit trail — the system log showing which user viewed, changed or printed each part of a chart.

Patient Confidentiality and Health Records Privacy Day by Day

Day 1: The Confidentiality Duty in Clinical Settings

- Professional Duty of Confidence — Boundaries for Clinicians and Support Staff
- Health Information Lifecycle Map — From Registration to Archive and Disposal
- Sensitive Record Categories — Mental Health, Genetics, Reproductive and Infectious Disease
- Patient Expectations and Trust — Why Disclosure Fears Change Clinical Candour
- Department Record Inventory — Paper Charts, Clinical Systems and Imaging Archives

Day 2: Lawful Use and Sharing of Records

- Purpose Tests for Disclosure — Direct Care Versus Secondary Uses
- Consent and Its Exceptions — Safeguarding, Public Health and Court Orders
- Referral and Discharge Letters — Sending Only What the Receiver Needs
- Insurer and Employer Requests — Verifying Authority Before Any Release
- Research Extracts and Pseudonymisation — Approving Studies Without Exposing Identities

Day 3: Access Controls for Clinical Systems

- Role-Based Chart Access Design — Matching Views to Ward and Specialty
- Break-the-Glass Procedures — Justifying and Reviewing Emergency Overrides
- Access Audit Trail Reviews — Spotting Curiosity Browsing and Celebrity Charts
- Joiner, Mover and Leaver Accounts — Closing Access When Staff Change Roles
- Workstation and Mobile Device Habits — Screen Locks, Printing and Messaging Apps

Day 4: Patient Rights and Confidentiality Incidents

- Patient Access Request Routine — Identity Checks, Redaction and Response Times
- Correction and Restriction Requests — Amending Charts Without Losing Clinical History
- Disclosure to Relatives and Carers — Proxy Authority and Capacity Questions
- Confidentiality Incident Triage — Misdirected Letters, Lost Files and Inappropriate Viewing
- Breach Notification and Learning Review — Informing Patients and Preventing Recurrence

Day 5: Practising the Patient Confidentiality Control Plan

- Department Lifecycle Map Check — Applying Day 1 Inventory to Live Records
- Disclosure Decision Exercises — Applying Day 2 Purpose Tests to Real Requests
- Access Profile Walkthrough — Testing Day 3 Roles Against Rota Patterns
- Retention and Secure Disposal Schedule — Periods for Each Record Type
- Patient Confidentiality Control Plan — Completing and Presenting the Department Plan

Applying Patient Confidentiality and Health Records Privacy After the Course

- Lead a monthly audit trail review, following up every unexplained chart view.
- Run a release-of-information check on the last twenty disclosures against the purpose tests.

Patient Confidentiality and Health Records Privacy Questions FAQ

What is patient confidentiality and health records privacy, and why does it matter now?

It is the set of duties and controls that keep what patients disclose limited to those caring for them. It matters now because shared clinical systems and outside requests have multiplied the ways a chart can be opened or released.

Which roles gain most from patient confidentiality and health records privacy training?

Health records, clinical governance and patient services staff gain most. Their daily decisions on copies, access and requests set how well a department protects its charts.

How does patient confidentiality and health records privacy differ from a general data privacy course?

It is grounded in clinical settings rather than general business records. It covers break-the-glass access, proxy authority and research pseudonymisation, with examples from hospitals and health insurers.

What do you bring back from patient confidentiality and health records privacy training?

You bring back a control plan for one department. It sets disclosure rules, access profiles, audit review routines, a patient request process, an incident response and a disposal schedule your governance committee can adopt.

Patient Confidentiality and Health Records Privacy: The Way Forward

The patient confidentiality control plan first informs which staff roles keep access to full charts and which see summaries only. Records officers, governance leads and system administrators use it whenever a role, ward or outside partner changes. After first use, revisit the break-the-glass section, since emergency overrides tend to become habits.