Institute of Health – Student Data Compliance Manual

Purpose & Disclaimer

This manual provides IOH students with a step-by-step framework to meet data protection and privacy standards as Functional Health Practitioners.
It is **educational only** and does not constitute legal advice.
Each practitioner is individually responsible for compliance with laws in their jurisdiction.

Quick Start – Core Principles

- Always operate with **consent, transparency, and security**.
- Collect only what is **necessary for care**.
- Store and share client data using **secure, compliant platforms**.
- Provide clients with **clear rights and choices**.
- Prepare in advance for **breaches, complaints, and audits**.

Step-by-Step Compliance Framework

Step 0: Know Your Legal Requirements

- **Australia**: Privacy Act 1988, 13 APPs, NDB scheme → see oaic.gov.au.
- **US**: HIPAA if covered entity/BA → Notice of Privacy Practices, BAA, safeguards, breach notification.
- **EU/UK**: GDPR/UK GDPR applies if you serve EU/UK clients → lawful basis, privacy notices, rights, DPAs, breach reporting in 72h.

Step 1: Client Consent

- Written, informed consent for all data collection.
- Must explain what, why, how, where, and for how long.
- Separate **offshore storage consent** where relevant.

Step 2: Minimal Data Collection

- Collect only what is relevant to client care and program delivery.

Step 3: Secure Software Use

- Approved platforms only (encrypted, DPA/BAA signed).
- Free Gmail/Dropbox/Notion **not permitted** for health data unless upgraded.
- **Australia**: APP 8 requires explicit consent for overseas storage.

Step 4: Google Workspace Compliance

- **US/HIPAA**: sign BAA.
- **EU/AU**: confirm DPA acceptance in Admin Console.
- Save a copy of terms for records.

Step 5: Security Configuration

- Enable 2FA for all accounts.
- Turn on audit logs and access monitoring.
- Block unverified third-party apps.
- Restrict file sharing outside your organisation.
- Configure Vault retention & deletion policies.
- Encrypt sensitive email (e.g., Virtru).

Step 6: Devices & Files

- Encrypt devices (FileVault, BitLocker).
- Use secure backups (Sync.com, Tresorit).
- Password-protect exported reports/PDFs.

Step 7: Privacy Policy

- Must be provided to every client.
- Must cover: collection, purpose, storage, sharing, overseas transfer, access/correction, complaints.

Step 8: Client Rights

- Provide processes for:
    - Data access requests
    - Correction of errors
    - Deletion where legally/clinically appropriate

Step 9: Data Retention

- Retain only as long as required.
- **Australia**: Adults – 7 years after last entry; Under 18 – until age 25.

Step 10: Breach Response

- Notify affected clients immediately.
- **GDPR**: 72h regulator notice.
- **HIPAA**: notify HHS + clients within 60 days.
- **Australia**: notify OAIC ASAP, ideally <30 days.

Step 11: Data Mapping

Maintain a private log of:

- Types of data collected
- Purpose
- Storage location
- Access roles
- Retention schedule
- Sharing arrangements

Step 12: Agreements

- **GDPR**: DPA required.
- **AU**: DPA recommended.
- **US**: BAA required if HIPAA applies.

Step 13: Notice of Privacy Practices

- HIPAA requirement only.
- More detailed than Privacy Policy, must include a complaints process.

Step 14: Staff & Admin

- Confidentiality agreements.
- Privacy/security training.
- Annual refreshers logged.

Step 15: HIPAA Safeguards (US only)

- Administrative → policies, training, logs.
- Physical → locks, controlled access.
- Technical → encryption, unique logins.

Appendices (Student Templates)

A1: Data Map Template

Data Type	Purpose	Storage	Access	Retention	Disposal
Intake forms	Care planning	Google Drive (AU/EU/US)	Practitioner	7 years/age 25	Secure deletion

---

A2: Retention Schedule

Record	Period	Trigger	Disposal Method
Adult case notes	7 years	Last entry	Shred/Wipe
Minor case notes	Until 25th birthday	Last entry	Shred/Wipe

A3: Sample Offshore Storage Consent

“This data may be stored on Google servers located in the United States or EU. Do you consent to this?” ☐ Yes ☐ No

---

A4: Incident Log Template

Date	Event	Data Affected	Action Taken	Notifications	Closed

A5: Practitioner Checklist (Onboarding)

☑ Consent obtained
☑ Privacy Policy shared
☑ Offshore consent (if applicable)
☑ Secure platform confirmed (DPA/BAA signed)
☑ Record entered in Data Map
☑ Retention tag applied

Student Assessment Requirement

Students must demonstrate:

- Reading and understanding of IOH Data Standards
- Informed consent captured for all assessments
- Privacy Policy and disclaimers issued
- Use of secure, approved storage systems
- Retention and deletion practices followed
- Ability to prepare a breach response if needed

Reading of this Data Compliance Manual is mandatory for IOH certification.
