HEALTHBRIDGE OCCUPATIONAL HEALTH CONFIDENTIALITY POLICY

1. POLICY STATEMENT

HealthBridge safeguards all personal and medical data per:

-UK GDPR & Data Protection Act 2018

-GMC Confidentiality Guidelines

-Faculty of Occupational Medicine Standards

-ISO 27001 (Information Security Management – *see definition below*)

What is ISO 27001?

ISO 27001 is the international standard for **Information Security Management Systems (ISMS)**. It requires:

-Risk-based protection of data (e.g., encryption, access controls).

-Regular audits and continuous improvement.

-Staff training on security protocols.

Relevance to This Policy:

Sections 4.1 (Data Handling), 7 (Breach Management), and 9 (Technical Safeguards) align with ISO 27001 controls.

---

2. SCOPE

Applies to:

-All staff, contractors, and third parties handling HealthBridge data.

-All data types: Electronic, paper, verbal, or visual (e.g., video consultations).

3. CONFIDENTIAL INFORMATION DEFINITION

Category	Examples
Clinical Data	OH reports, GP letters, medication lists.
Employee Records	HR files, absence histories.
Commercial Data	Contracts, pricing, business strategies.
Identifiers	NHS numbers, email/phone, job titles.

4. CORE PRINCIPLES

4.1 DATA HANDLING

-**Need-to-know access**: Role-based permissions (e.g., clinicians vs. admin).

-**Minimum necessary disclosure**: Redact non-relevant details in shared reports.

-**Encryption**: Mandatory for emails/cloud storage (AES-256 standard).

4.2 CONSENT AND TRANSPARENCY

-**Explicit consent** required for employer report sharing (except legal exemptions).

-**Privacy notices** explain data use (e.g., website, consultation intake forms).

5. PERMITTED DISCLOSURES WITHOUT CONSENT

Disclosures are lawful only if:

- **Safeguarding**: Risk of harm to self/others (per GMC para 26).

-**Legal order**: Court subpoena or statutory requirement (e.g., RIDDOR).

-**Public interest**: Rare cases (e.g., pandemic response).

Note: Document all non-consensual disclosures with rationale.

---

6. STAFF ACCOUNTABILITY

6.1 MANDATORY MEASURES

-Annual training: GDPR, phishing awareness, OH confidentiality.

-Contract clauses: Confidentiality agreements for all hires.

-Access logs: Monthly audits of EHR/system access.

6.2 MANAGER DUTIES

-Quarterly spot-checks: 5% of randomly selected cases.

-Breach drills: Simulated incidents biannually.

---

7. BREACH MANAGEMENT

7.1 REPORTING

Severity	Action
Suspected breach	Report to DPO within **1 hour**.
High-risk breach	ICO notified within **72 hours**.

7.2 CONSEQUENCES

-Staff: Disciplinary action up to termination.

-Contractors: Contract termination.

-Legal*:* Fines are proportionate to the breach severity and organizational size. HealthBridge implements cost-effective safeguards to minimize risks.

---

8. PATIENT RIGHTS

-Subject Access Requests: Fulfilled within 1 month (no fee unless excessive).

-Data Correction: Update inaccuracies within 14 days.

-Complaints: Escalate to ICO if unresolved internally.

---

9. TECHNICAL SAFEGUARDS (ISO 27001 CONTROLS)

Data Type	Protection Method
Digital	AES-256 encryption, MFA, auto-logoff (15 mins).
Verbal	Private rooms for calls; no names in public areas.

---

10. REVIEW & GOVERNANCE

-Annual review by Data Protection Officer & Clinical Lead.

-Trigger updates: New legislation (e.g., post-Brexit GDPR changes).

Contact for Breaches: [contact@healthbridge.org.uk]

11. VERSION CONTROL

Version	Date	Changes Made	Approved By
1.0	30/07/2025	Initial policy draft.	Dr. James Stanley
1.1	[DD/MM/YYYY]		

Approved by: Dr. James Stanley

Contact: [contact@healthbridge.org.uk]