# HEALTHBRIDGE OCCUPATIONAL HEALTH MEDICAL RECORDS RETENTION POLICY

## 1. POLICY PURPOSE

To ensure:

-Legally compliant retention of OH records per:

**~UK GDPR (Article 5)** & **DPA 2018**

**~Faculty of Occupational Medicine (FOM) Guidelines** (2023)

**~GMC Good Medical Practice** (2024)

-Secure, auditable storage and disposal aligned with **ISO 27001** (Information Security).

---

## 2. SCOPE & APPLICABILITY

| Record Type | Examples | Custodians |
|---|---|---|
| Clinical Records | OH reports, consultation notes | OH Practitioners |
| Employer Data | Referrals, workplace adjustments | HR/Admin |
| Operational Logs | Access audits, disposal certificates | Data Protection Officer |

**Applies to**: All staff, contractors, and third-party processors.

---

 © HealthBridge. Unauthorized distribution prohibited.

## 3. RETENTION SCHEDULE

| Record Type | Retention Period | Legal Basis | Exception Triggers |
|---|---|---|---|
| OH Reports | 40 years post-last entry | FOM Standard | Ongoing litigation |
| Referrals | 6 years post-case closure | Limitation Act 1980 | Safeguarding concerns |
| Complaints | 10 years post-resolution | NHS Digital Code | ICO investigation |
| Consent Forms | 10 years | UK GDPR (Article 7) | N/A |

---

## 4. STORAGE & SECURITY PROTOCOLS

### 4.1 DIGITAL RECORDS

**Encryption**:

-At rest: AES-256 (BitLocker/FileVault).

-In transit: TLS 1.2+ (e.g., NHSmail standards).

**Access Control**:

-Role-based permissions (reviewed quarterly).

-MFA required for remote access.

**Audit Trails**:

-Log all accesses (user, date, purpose) - retained for **3 years**.

### 4.2 PAPER RECORDS

 © HealthBridge. Unauthorized distribution prohibited.

-Stored in locked cabinets (BS EN 1303-certified locks).

-Shredded via **confidential waste provider** (certificate of destruction retained).

---

## 5. DISPOSAL PROCESS

| Medium | Method | Standard |
|---|---|---|
| Digital | Secure deletion (Eraser, DoD 5220.22-M) | ISO 27001 Annex A.8.10 |
| Paper | Cross-cut shredding (≤6mm particles) | DIN 66399 Level 3 |

**Verification**:

-IT Manager confirms deletion via log.

-DPO spot-checks 5% of disposals annually.

---

## 6. SUBJECT ACCESS & AMENDMENTS

### 6.1 SAR WORKFLOW

**1. Request Received**: Logged in SAR register (date, requester, scope).

**2. Verification**:

-ID checked (passport + utility bill).

-Third-party data redacted per GMC guidelines.

**3. Delivery**:

-Encrypted email (Password: SMS'd separately).

-Portal access (15-day expiry).

 © HealthBridge. Unauthorized distribution prohibited.

### 6.2 EMPLOYEE RIGHTS

**Corrections**: Amend inaccuracies within **14 days**.

**Restrictions**: Flag disputes in EHR (halts processing).

---

## 7. ROLES & ACCOUNTABILITY

| Role | Key Duties |
|---|---|
| Data Protection Officer | Annual audits, ICO breach reporting (≤72h). |
| OH Lead | Clinician training on redaction/disposal. |
| IT Manager | Enforce encryption, access logs. |

---

## 8. GOVERNANCE & REVIEW

**Quarterly**: Spot-checks (5% records).

**Annual**: Full audit against ISO 27001 Annex A.8.

**Triggers**: New case law (e.g., *Lloyd v Google*), ICO guidance.

**Breach Contact**: [contact@healthbridge.co.uk]

---

 © HealthBridge. Unauthorized distribution prohibited.

## 9. 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]

 © HealthBridge. Unauthorized distribution prohibited.