DATA MANAGEMENT POLICY

HealthBridge Corp

Document Ref: HBC-DM-POL-001 | Version: 2.0 | Classification: CONFIDENTIAL

Version Control

Version	Date	Author	Description	Status
1.0	05 Apr 2022	P. Okafor (CDO)	Initial policy. Covers data inventory, classification, retention.	Approved
1.1	12 Sep 2022	P. Okafor (CDO)	Added DSAR procedure following EU DPA inquiry notification.	Approved
2.0	08 Jan 2024	P. Okafor (CDO)	Major revision. Added vendor section. Updated HIPAA retention tables.	Approved

Approval and Sign-Off

Role	Name	Signature	Date
Chief Executive Officer	K. Adeyemi	_____	08 Jan 2024
Chief Data Officer	P. Okafor	_____	08 Jan 2024
Data Protection Officer		_____	
Legal Counsel		_____	
Head of Information Security		_____	

GAP: The DPO, Legal Counsel, and Head of Information Security sign-off columns are all blank. GDPR Article 37 requires a DPO where large-scale processing of special category data occurs — HealthBridge processes 2.4M patient records. DPO review and approval of this policy is a regulatory obligation, not optional.

1. Purpose

HealthBridge Corp ("HealthBridge" or "the Organisation") processes personal data and protected health information (PHI) on behalf of healthcare providers across the European Union and United States. This policy establishes requirements for the management, protection, classification, retention, and disposal of data assets to ensure compliance with the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and applicable national data protection laws including the Nigerian Data Protection Act (NDPA) 2023. Effective data management is foundational to patient safety, regulatory compliance, and organisational trust.

2. Scope

This policy applies to all HealthBridge employees, contractors, and third-party processors who handle personal data or PHI in any form — electronic, physical, or verbal. It covers all systems, databases, and storage media operated by or on behalf of HealthBridge.

> **AUDIT NOTE — DELIBERATE GAP**
> *SCOPE GAP: This policy does not explicitly address personal data processed by HealthBridge employees using personal devices (BYOD). No mobile device management (MDM) policy is referenced. PHI accessed via personal smartphones or laptops falls outside the current control framework.*

3. Data Classification

All data assets must be classified according to the following scheme:

Classification	Description	Examples	Handling Requirements
Public	Approved for external release	Marketing content, published reports	No restrictions
Internal	Business use only, not for external sharing	Internal communications, project plans	Access controls, no external sharing
Confidential	Restricted; encryption required at rest and in transit	Financial data, HR records, contracts	Encryption, access logging, NDA for third parties
Restricted (PHI/PII)	Highest protection; access on strict need-to-know	Patient records, biometric data, diagnosis codes	AES-256 encryption, MFA, audit logging, BAA/DPA required

> **AUDIT NOTE — DELIBERATE GAP**
> *CLASSIFICATION GAP: This policy defines classification levels but does not require data assets to be labelled with their classification at creation. No technical labelling controls (e.g. Microsoft Purview, metadata tagging) are referenced. Classification relies entirely on individual judgement with no verification mechanism.*

4. Data Inventory

HealthBridge shall maintain a Data Asset Register (DAR) covering all personal data and PHI processed by the Organisation. The register must include:

- Data category and description
- Legal basis for processing (GDPR Article 6 / Article 9)
- Storage location and system name
- Data controller / data processor designation
- Retention period and deletion schedule
- Cross-border transfer details (where applicable)

- Third-party processors with access

AUDIT NOTE — DELIBERATE GAP

DATA INVENTORY GAPS: (1) No owner is assigned to maintain the DAR — responsibility is collective, meaning it is no one's responsibility. (2) No update frequency is specified. GDPR Article 30 requires records of processing activities to be kept up to date. (3) Data flows between systems are not required to be documented in the register. A system may receive PHI from another system without this transfer being captured. (4) The DAR template and storage location are not referenced in this policy.

5. Data Retention and Disposal

Data must be retained only for as long as necessary for the purpose for which it was collected, subject to the minimum periods below:

Data Category	Minimum Retention	Legal Basis	Maximum / Delete By
Patient Records (PHI)	6 years from last treatment	HIPAA 45 CFR §164.530	Not defined in this policy
Employee HR Records	7 years from termination	EU Labour Law / Employment Act	Not defined in this policy
Financial Records	7 years	Companies Act 2006	Not defined in this policy
Audit Logs	1 year	Internal Policy	Not defined in this policy
Marketing Contacts (EU)	Duration of consent	GDPR Art.5(1)(e)	Upon consent withdrawal
DSAR Records	3 years from response date	ICO Guidance	Not defined in this policy
Incident Records	5 years	Internal Policy / Insurance	Not defined in this policy

AUDIT NOTE — DELIBERATE GAP

RETENTION GAPS: (1) Minimum retention periods are defined but maximum retention periods and deletion deadlines are absent. GDPR's storage limitation principle (Art.5(1)(e)) requires data not be kept longer than necessary. (2) "6 years from last treatment" for PHI does not align precisely with HIPAA, which requires 6 years from the date of creation OR the date it was last in effect, whichever is later. (3) "Duration of consent" for marketing contacts is vague — there is no process to verify when consent was withdrawn or to trigger deletion. (4) No automated deletion mechanism is required or referenced. Deletion relies entirely on manual action.

5.2 Data Disposal

When data reaches end of retention, it must be securely deleted. Electronic data must be overwritten in accordance with NIST SP 800-88 standards or cryptographically erased. Physical media must be shredded or degaussed by an approved vendor.

AUDIT NOTE — DELIBERATE GAP

DISPOSAL GAPS: (1) No certificate of destruction is required from disposal vendors. (2) No verification process exists to confirm deletion was completed. (3) No requirement to update the Data Asset Register upon deletion to reflect that the data no longer exists. (4) No process for deleting data from backup media once the primary data has been deleted.

6. Data Subject Rights

HealthBridge must facilitate the following data subject rights under GDPR Chapter III:

Right of Access (DSAR): Respond within 30 days. Log all requests. Dedicated inbox: privacy@healthbridge.com

Right to Rectification: Correct inaccurate data within 30 days of request

Right to Erasure: Assess against legitimate grounds; respond within 30 days

Right to Restriction: Restrict processing pending resolution of disputes

Right to Portability: Provide data in machine-readable format within 30 days

Right to Object: Cease processing for direct marketing immediately upon objection

> **AUDIT NOTE — DELIBERATE GAP**
> *DSAR GAPS: (1) No process exists to verify the identity of the requestor before releasing personal data — this creates a risk of disclosure to an unauthorised third party. (2) No escalation path is defined for complex requests that cannot be completed within 30 days (GDPR permits a 2-month extension with notice). (3) No requirement to track the source, volume, or nature of DSARs for trend analysis or regulatory reporting. (4) The policy does not address how to handle DSARs received verbally or via social media channels.*

7. Encryption and Technical Controls

All Restricted (PHI/PII) data stored on HealthBridge systems must be encrypted using AES-256 or equivalent. All Confidential and Restricted data transmitted over any network must be encrypted using TLS 1.2 or higher.

> **AUDIT NOTE — DELIBERATE GAP**
> *ENCRYPTION GAPS: (1) This policy does not address encryption of data on portable media (USB drives, laptops). Unencrypted PHI on a lost laptop would constitute a notifiable breach. (2) No key management policy is referenced — who holds encryption keys, how often they are rotated, and what happens when a key holder leaves is undefined. (3) TLS 1.2 is the minimum stated — TLS 1.3 is now the industry standard and should be the baseline for new implementations.*

8. Third-Party and Vendor Management

All vendors and third parties that process personal data or PHI on behalf of HealthBridge must sign a Data Processing Agreement (DPA) before processing begins. US vendors handling PHI must also execute a Business Associate Agreement (BAA). Vendor risk ratings must be assigned before onboarding.

> **AUDIT NOTE — DELIBERATE GAP**
> *VENDOR GAPS: (1) No security assessment is required before vendor onboarding — a vendor may sign a DPA and begin processing PHI without demonstrating any security capability. (2) No ongoing compliance monitoring is required — once onboarded, vendor controls are not re-assessed unless a breach occurs. (3) Sub-processors: this policy is silent on whether vendors may engage sub-processors without HealthBridge notification or approval. GDPR Article 28(2) requires controller authorisation for sub-processing. (4) No requirement to review vendor SOC 2 reports, ISO 27001 certificates, or equivalent third-party assurance.*

9. Data Breach Notification

Suspected data breaches must be reported to the Data Protection Officer (DPO) within 24 hours of discovery. Where a breach is likely to result in a risk to the rights and freedoms of data subjects, HealthBridge must notify the relevant supervisory authority within 72 hours (GDPR Article 33). Where a breach is likely to result in a high risk to data subjects, affected individuals must be notified without undue delay (GDPR Article 34).

AUDIT NOTE — DELIBERATE GAP

BREACH NOTIFICATION GAPS: (1) No breach severity classification framework exists — the determination of "likely risk" and "high risk" thresholds is subjective and unguided. (2) No breach response runbook or playbook is referenced. (3) No requirement for breach simulation exercises or tabletop testing of the notification procedure. (4) The 72-hour regulatory notification clock begins from when the Organisation "becomes aware" — no process exists to define when awareness is formally established, which could delay the clock.

10. Policy Review

This policy is reviewed annually by the Chief Data Officer. The next scheduled review is January 2025. Material changes to the regulatory landscape or the Organisation's data processing activities may trigger an interim review.