PRIVACY & DATA SUBJECT RIGHTS POLICY

HealthBridge Corp

Document Ref: HBC-PRIV-POL-001 | Version: 1.2 | Classification: CONFIDENTIAL

Version Control

Version	Date	Author	Description	Status
1.0	01 Jun 2022	P. Okafor (CDO)	Initial policy following GDPR readiness review.	Approved
1.1	15 Nov 2022	K. Eze (Legal)	Updated to reflect EU DPA inquiry. Added HIPAA breach obligations.	Approved
1.2	10 Jan 2024	P. Okafor (CDO)	Added NDPA 2023 section. Updated privacy notice requirements.	Approved

Approval and Sign-Off

Role	Name	Signature	Date
Chief Executive Officer	K. Adeyemi	_____	10 Jan 2024
Data Protection Officer		_____	
Legal Counsel	K. Eze	_____	10 Jan 2024
Chief Data Officer	P. Okafor	_____	10 Jan 2024

GAP: The Data Protection Officer signature is missing. GDPR Article 39 requires the DPO to be involved in all matters relating to the protection of personal data. A privacy policy approved without DPO sign-off may not satisfy supervisory authority requirements.

1. Purpose and Regulatory Framework

This policy governs HealthBridge Corp's approach to privacy, the exercise of data subject rights, and compliance with applicable privacy regulations including: GDPR (EU) 2016/679, HIPAA (US) 45 CFR Parts 160 and 164, the Nigerian Data Protection Act (NDPA) 2023, and applicable national implementing legislation.

2. Privacy by Design and Default

HealthBridge is committed to embedding privacy considerations into the design of all new systems, processes, and services from inception. All new data processing activities involving personal data must undergo a Privacy Impact Assessment (PIA) before implementation.

> **AUDIT NOTE — DELIBERATE GAP**
> *PRIVACY BY DESIGN GAP: No formal PIA process, template, or completion threshold is defined in this policy or any referenced procedure. The requirement to conduct a PIA exists, but without a defined process, PIAs may be inconsistently applied or omitted entirely without detection.*

3. Legal Basis for Processing

HealthBridge must identify and document a valid legal basis for each category of personal data processed. The applicable legal bases under GDPR Article 6 and Article 9 are:

Article 6(1)(a) — Consent: Freely given, specific, informed, and unambiguous consent from the data subject

Article 6(1)(b) — Contract: Processing necessary for performance of a contract with the data subject

Article 6(1)(c) — Legal Obligation: Processing necessary for compliance with a legal obligation

Article 6(1)(f) — Legitimate Interests: Processing necessary for legitimate interests, subject to balancing test

Article 9(2)(h) — Healthcare: Processing of special category data for healthcare purposes by health professionals

> **AUDIT NOTE — DELIBERATE GAP**
> *LEGAL BASIS GAP: This policy requires a legal basis to be documented but does not specify where or how this documentation is maintained. Legal basis records are not linked to the Data Asset Register. An audit of processing activities would likely find undocumented or post-hoc legal basis assignments.*

4. Privacy Notices

HealthBridge must provide clear and transparent privacy notices to data subjects at the point of data collection. Notices must include all information required under GDPR Articles 13 and 14 and must be written in plain language accessible to the intended audience.

5. Consent Management

Where consent is used as the legal basis for processing, it must be: freely given (not bundled or coerced), specific (for a defined purpose), informed (after reading the privacy notice), unambiguous (clear affirmative action), and withdrawable (as easily as it was given).

> **AUDIT NOTE — DELIBERATE GAP**
> *CONSENT GAPS: (1) No consent management platform or register is referenced. Proof of consent must be retained but no storage mechanism is defined. (2) No process exists to withdraw consent systematically across all systems — a data subject who withdraws consent may still receive processing in systems not connected to the consent record.*

6. Data Subject Rights Procedure

All data subject rights requests must be acknowledged within 5 business days of receipt and fulfilled within 30 calendar days. Requests received at privacy@healthbridge.com are logged in the DSAR tracker by the Data Protection Officer (or designated deputy).

Right	Response Deadline	Process Owner	Extension Possible?
Right of Access	30 days	DPO	Yes — 2 months (with notice)
Right to Rectification	30 days	DPO + System Owner	Yes — 2 months (with notice)
Right to Erasure	30 days	DPO + IT	No (unless complex search)
Right to Restriction	Without undue delay	DPO + IT	No
Right to Portability	30 days	DPO + IT	Yes — 2 months
Right to Object	Immediately (direct marketing)	DPO + Marketing	No (marketing objections)

AUDIT NOTE — DELIBERATE GAP

DSAR PROCEDURE GAPS: (1) No identity verification procedure before disclosing personal data. A malicious actor could submit a DSAR impersonating a data subject. (2) No escalation process for manifestly unfounded or excessive requests (GDPR Art.12(5)). (3) DPO column is the named process owner, but the DPO sign-off on this policy is absent — the named owner has not agreed to this responsibility.

7. Cross-Border Data Transfers

Transfers of personal data to countries outside the European Economic Area (EEA) must be subject to appropriate safeguards including: adequacy decisions, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other approved transfer mechanisms.

AUDIT NOTE — DELIBERATE GAP

TRANSFER GAP: HealthBridge operates across EU and US jurisdictions. The legal transfer mechanism for EU-to-US transfers must be documented — EU-US Data Privacy Framework adequacy decision applies only to certified US organisations. No certification status for HealthBridge US operations is referenced in this policy.

8. Data Breach — Privacy Obligations

In the event of a personal data breach: (a) notify the DPO within 24 hours; (b) notify the supervisory authority within 72 hours if risk to data subjects exists (GDPR Art.33); (c) notify affected data subjects without undue delay if high risk exists (GDPR Art.34); (d) for PHI breaches, notify HHS (US) and affected individuals per HIPAA Breach Notification Rule within 60 days of discovery.

9. Policy Review

This policy is reviewed annually. Next review: January 2025.