Data and Privacy Management Policy

---

1. Introduction

At AMBHC, we are committed to protecting the privacy and security of all personal information we collect, store, and process. In addition to the protections guaranteed under HIPAA, this policy outlines how we collect, use, safeguard, and share personal data for both Clients and employees.

---

2. Types of Information Collected

- **Client Data:** Identifiers (name, date of birth, address), health and diagnosis information, contact details (phone, email), and service-related notes.
- **Employee Data:** Identifiers, employment records, credentials, and payroll information.
- **System Access Data:** Usernames, passwords, access logs, and device identifiers.

---

3. How Information Is Collected

- **Directly from Individuals:** During intake, onboarding, and routine care interactions.
- **Electronically:** Via our secure portal, mobile applications, and electronic health record (EHR) systems.
- **Third-Party Referrals:** From hospitals, physicians, or community partners, with proper consent.

---

4. Purpose of Data Collection

- **Care Coordination:** To plan, deliver, and document high-quality home care services.
- **Payment & Administration:** To process payroll, billing, and regulatory reporting.
- **Quality Improvement:** To monitor outcomes, audit performance, and drive staff training.
- **Compliance:** To meet legal, regulatory, and accreditation requirements.

---

5. Data Security Measures

- **Physical Protections:** Hard-copy records are stored in locked, access-controlled areas.
- **Technical Controls:**
    - All electronic files reside on a password-protected, encrypted server.

    - Devices accessing sensitive data must have up-to-date antivirus software and full-disk encryption.
    - Passwords are changed at least every three months, and multi-factor authentication is enforced where available.
- **Administrative Safeguards:** Semi-annual training on data security best practices and emerging technology risks for all staff.

---

6. Data Sharing Practices

- **Internal Sharing:** Access is limited to authorized personnel on a need-to-know basis.
- **External Sharing:** We do not share personal data with third parties, except as required by law (e.g., reporting a breach to the Pennsylvania Department of Human Services Office for Civil Rights or cooperating with state police).
- **SMS Consent:** "SMS consent and phone numbers will never be shared with third parties or affiliates under any circumstances."

---

7. User Rights

Clients and employees have the right to:

- Access and obtain a copy of their personal data.
- Request correction of inaccurate or incomplete information.
- Request deletion or restriction of processing where applicable.
- Withdraw consent for communications (including SMS) at any time, without impacting care or employment.

---

8. In the Event of a Data Breach

Should a breach occur—whether through malicious attack or accidental loss—AMBHC will:

1. **Immediate Response:** Contain and mitigate the incident, engaging external experts as needed.
2. **Notification:**
    - Inform the Pennsylvania Department of Human Services Office for Civil Rights.
    - Notify state police within two hours of discovery.
    - Notify affected individuals within 48 hours.
3. **Investigation & Remediation:** Identify the root cause, secure systems, and produce a full incident report within 60 days.