[Your Practice/Organization Name]

HIPAA Privacy Policy

Effective Date: [Date]

1.0 Purpose & Scope

This document establishes the official internal policy for the protection of Patient Health Information (PHI) for **[Your Practice/Organization Name]**. This policy applies to all members of our workforce, including employees, volunteers, trainees, and other persons whose conduct, in the performance of work for our organization, is under our direct control. This policy is enacted to ensure full compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and all other applicable federal and state laws.

2.0 Definitions

- **Protected Health Information (PHI):** Any individually identifiable health information created, received, maintained, or transmitted by our organization, regardless of form (e.g., electronic, paper, oral). This includes demographic data, medical histories, test results, insurance information, and other data that could identify a patient.
- **Covered Entity (CE):** As a healthcare provider that conducts certain financial and administrative transactions electronically, **[Your Practice/Organization Name]** is a Covered Entity under HIPAA.
- **Business Associate (BA):** A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, our organization.
- **Workforce:** All employees, volunteers, trainees, and other persons under the direct control of **[Your Practice/Organization Name]**.
- **Treatment, Payment, and Healthcare Operations (TPO):**
    - **Treatment:** The provision, coordination, or management of health care and related services.
    - **Payment:** Activities undertaken to obtain reimbursement for services, including billing, claims management, and eligibility determination.
    - **Operations:** Administrative, financial, legal, and quality improvement activities necessary to run our business.

3.0 Policy: Permitted Uses and Disclosures of PHI

3.1 Without Patient Authorization: We may use and disclose PHI without a patient's written authorization for the purposes of Treatment, Payment, and Healthcare Operations (TPO).

3.2 With Patient Authorization: Any use or disclosure of PHI for purposes other than TPO requires a specific, written authorization from the patient. This includes, but is not limited to, most uses and disclosures for marketing purposes or the sale of PHI.

3.3 Minimum Necessary Standard: We will make reasonable efforts to limit the use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose.

4.0 Patient Rights

All patients of **[Your Practice/Organization Name]** have the following rights regarding their PHI:

- **Right to Access:** To inspect and obtain a copy of their PHI.
- **Right to Amend:** To request an amendment to their PHI if they believe it is inaccurate or incomplete.
- **Right to an Accounting of Disclosures:** To receive a list of certain disclosures we have made of their PHI.
- **Right to Request Restrictions:** To request a restriction on certain uses and disclosures of their PHI.
- **Right to Confidential Communications:** To request that we communicate with them about their health information in a specific way or at a certain location.
- **Right to a Paper Copy of the Notice of Privacy Practices (NPP):** To receive a paper copy of our patient-facing NPP at any time.

5.0 Safeguards for Protecting PHI

[Your Practice/Organization Name] will implement and maintain the following safeguards to protect PHI:

- **Administrative Safeguards:**
    - Designation of a Privacy Officer: **[Name of Privacy Officer]**.
    - A formal sanctions policy for workforce members who fail to comply with this policy.
    - A mandatory, documented training program for all workforce members on privacy and security policies.
    - Regular risk assessments to identify and mitigate potential vulnerabilities.
- **Physical Safeguards:**
    - Securing all physical records containing PHI in locked cabinets or rooms.
    - Implementing policies for workstation use and security to prevent unauthorized viewing of PHI.
    - Controlling and monitoring physical access to facilities where PHI is stored.
- **Technical Safeguards:**
    - Implementing access controls (e.g., unique user IDs, passwords) for all systems containing electronic PHI.
    - Using encryption to protect electronic PHI where appropriate.

- Maintaining audit logs and regularly monitoring system activity.

6.0 Breach Notification Procedures

In the event of a breach of unsecured PHI, **[Your Practice/Organization Name]** will follow its Breach Notification Policy, which includes procedures for timely notification to affected individuals, the Secretary of Health and Human Services, and, where applicable, the media, in accordance with the HIPAA Breach Notification Rule.

7.0 Privacy Officer

The designated Privacy Officer for **[Your Practice/Organization Name]** is:

Name: [Privacy Officer Name] **Title:** [Privacy Officer Title] **Contact Information:** [Email and/or Phone Number]

The Privacy Officer is responsible for the development, implementation, and oversight of this policy.

8.0 Policy Review and Updates

This policy will be reviewed at least annually and updated as needed to reflect changes in federal and state law, technology, and our organization's operations.

Workforce Member Acknowledgment

I, [Employee Name], acknowledge that I have received, read, and understand the **[Your Practice/Organization Name]** HIPAA Privacy Policy. I agree to abide by the terms of this policy as a condition of my employment/association with this organization.

Signature: _____

Printed Name: _____

Date: _____