



Patient Information Privacy Policy

Effective Date: November 10th, 2025

1.0 Purpose & Scope

This document establishes the official internal policy for the protection of Patient Health Information (PHI) for Integrated Behavioral Health. 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.

IBH respects your privacy. SMS Consent, and phone numbers collected for SMS communication purposes will not be shared with any third party or affiliates for marketing purposes. Patient phone numbers are collected through our Online New Patient Request & Demographics online patient intake form.

IBH will never release, sell, or otherwise distribute any of your contact information without your direct consent. You may opt out or opt in at any time. These messages are not for marketing purposes, only for streamlined healthcare communication.

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, Integrated Behavioral Health 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 Integrated Behavioral Health.
- 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.
- 3.4 Mandatory Reporting:** In certain situations where a patient has expressed a desire and plan to harm themselves or others, or if there is a signed bench order requesting patient information, we must provide the minimum necessary patient information.

4.0 Patient Rights

All patients of Integrated Behavioral Health 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

Integrated Behavioral Health will implement and maintain the following safeguards to protect PHI:

- Administrative Safeguards:**
 - Designation of a Privacy Officer: Ron Mason.
 - 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:**
 - Designation of a Security Officer: Mitch Wade.
 - 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, Integrated Behavioral Health 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 Integrated Behavioral Health is:

Name: Ron Mason **Title:** Director of Medical Records **Contact Information:** rmason@ibhus.com

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 annually and updated as needed to reflect changes in federal and state law, technology, and our organization's operations.