

# Privacy Practices and Procedures

Practice Name: Mental Wellness for the Human Experience, LLC

Address: 1224 Mill St, Bldg B, Suite 001, East Berlin, CT 06023

Phone: 860-348-5650

Effective Date: 1/07/2026

---

## Purpose

This document establishes the privacy practices and internal procedures for protecting patient health information in compliance with the Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act, and applicable Connecticut state laws. These practices apply to all workforce members, contractors, and trainees of the practice.

---

## Definitions

- PHI (Protected Health Information): Individually identifiable health information in any form.
- ePHI: PHI maintained or transmitted electronically.
- Workforce: Employees, contractors, interns, and volunteers.
- Minimum Necessary: Limiting use or disclosure of PHI to the least amount needed.

---

## Notice of Privacy Practices

### Our Legal Duties

We are required by law to maintain the privacy and security of your PHI, provide you with this Notice, and follow the terms described.

## **How We May Use and Disclose PHI**

We may use and disclose your PHI without your authorization for:

- Treatment: Coordination of care with other providers.
- Payment: Billing, claims, and utilization review.
- Health Care Operations: Quality improvement, supervision, training, and administrative activities.

## **Other Permitted or Required Uses**

- As required by law (e.g., reporting abuse or neglect)
- Public health and safety activities
- Health oversight activities
- Judicial or administrative proceedings
- Law enforcement purposes
- To prevent a serious threat to health or safety

## **Uses Requiring Authorization**

We will obtain your written authorization for uses not described above, including psychotherapy notes (with limited exceptions), marketing, and sale of PHI.

## **Your Rights**

You have the right to:

- Inspect and obtain a copy of your medical record

- Request corrections
- Request confidential communications
- Request restrictions (not always required to be agreed to)
- Receive an accounting of disclosures
- Obtain a paper or electronic copy of this Notice
- Be notified of a breach of unsecured PHI

## **Complaints**

You may file a complaint with the practice or the U.S. Department of Health and Human Services without fear of retaliation.

---

## **Internal Privacy Procedures**

### **Access Controls**

- Access to PHI is role-based and limited to job responsibilities
- Unique user IDs and strong passwords for all systems
- Automatic log-off for electronic systems when available

## **Safeguards**

### Administrative Safeguards

- Designated Privacy Officer
- Workforce training upon hire and annually
- Sanctions for violations

## Physical Safeguards

- Locked offices and file cabinets
- Screen privacy in shared areas
- Secure disposal of paper records via shredding

## Technical Safeguards

- Encrypted devices and email when transmitting ePHI
- Secure, HIPAA-compliant EHR and telehealth platforms
- Regular software updates

---

## Use and Disclosure Procedures

- Verify patient or authorized representative identity before releasing PHI.
- Apply the HIPAA minimum necessary standard to all disclosures.
- Use secure transmission methods (encrypted email, secure portals, or approved EHR tools).
- Disclosures are documented when required by HIPAA or Connecticut law.

## Connecticut-Specific Rules for Minors and Parental Access

- Connecticut law recognizes that minors may consent to certain types of care (including, but not limited to, mental health treatment under specific circumstances, substance use treatment, and reproductive health services).

- When a minor legally consents to their own treatment, the parent or guardian may not have automatic access to those records.
- Access to minor records is limited to what Connecticut law permits and what is clinically appropriate.
- Providers may deny parental access if disclosure would be reasonably likely to endanger the patient or compromise treatment, consistent with Connecticut statutes and HIPAA.
- All decisions regarding parental access are documented in the medical record.

## **Patient Requests Procedures**

- Record Requests: Fulfilled within 30 days (or 60 with written notice)
- Amendments: Respond within 60 days
- Accounting of Disclosures: Provided within 60 days
- Requests must be documented and logged

---

## **Telehealth and Electronic Communication**

- Telehealth services are provided using HIPAA-compliant platforms approved for use in Connecticut.
- Patients are informed of privacy risks associated with electronic communication and telehealth, including potential limitations of confidentiality.
- Email and text messaging are limited to scheduling, billing, and administrative purposes unless the patient provides written authorization.
- Telehealth services for minors comply with Connecticut consent and confidentiality laws, including documentation of parental consent when required.

---

## **Business Associates**

- Written Business Associate Agreements (BAAs) required
- Vendors are vetted for HIPAA compliance
- Ongoing monitoring as appropriate

---

## **Breach Notification Procedures**

- Immediate internal reporting of suspected breaches
- Risk assessment conducted promptly
- Notification to affected individuals without unreasonable delay and no later than 60 days
- Reporting to HHS and state authorities as required

---

## **Training and Sanctions**

- Initial and annual HIPAA training required
- Sanctions applied consistently based on severity
- Documentation of training and disciplinary actions maintained

---

## **Record Retention**

- Adult medical records are retained for a minimum of 7 years from the date of last service, in accordance with Connecticut General Statutes and professional standards.
- Minor records are retained for at least 7 years after the patient reaches the age of 18 (i.e., until at least age 25), consistent with Connecticut law and risk management guidance.
- Records involved in litigation, audits, or investigations are retained until final resolution, even if this extends beyond standard retention periods.
- All records are securely destroyed at the end of the retention period using HIPAA-compliant methods (shredding for paper; secure deletion for electronic records).

---

## **Privacy Officer Contact**

Phone: 860-348-5650

Address: 1224 Mill St, Bldg B, Suite 001, East Berlin, CT 06023

---