NOTICE OF PRIVACY PRACTICES
Complete and Detailed Version

MOSAIC BLOOM COUNSELING, LLC
Marquita Bolden, LCSW
8302 Old York Road, Suite B1 Elkins Park, PA 19027
Phone: 267-227-0122
Email: mbolden@mosaicbloomcounseling.com
Website: www.mosaicbloomcounseling.com

Licensed in Pennsylvania, Delaware, New Jersey, and Idaho

EFFECTIVE DATE: October 12, 2025

TABLE OF CONTENTS

---

1. INTRODUCTION: YOUR INFORMATION, YOUR RIGHTS, OUR RESPONSIBILITIES

This Notice of Privacy Practices describes how Mosaic Bloom Counseling, LLC may use and disclose your protected health information to carry out treatment, payment, or health care

operations, and for other purposes that are permitted or required by law. It also describes your rights regarding your health information and our legal responsibilities concerning that information.

Federal and state laws require us to:

- Maintain the privacy and security of your protected health information
- Provide you with this notice of our legal duties and privacy practices with respect to your health information
- Follow the terms of the notice currently in effect
- Notify you if we are unable to agree to a requested restriction on how we use or disclose your information
- Accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations

We reserve the right to change our practices and to make the new provisions effective for all protected health information we maintain. Should our information practices change, we will post a revised notice in our office and on our website at www.mosaicbloomcounseling.com. This notice is effective as of October 12, 2025.

Questions or concerns? Contact us at 267-227-0122 or mbolden@mosaicbloomcounseling.com

---

2. KEY DEFINITIONS

To help you understand this notice, here are some important terms:

Protected Health Information (PHI): Information in your health record that could identify you, including:

- Demographic information (name, address, date of birth, Social Security number)
- Medical history and presenting problems
- Mental health diagnoses
- Treatment plans and progress notes
- Test results and assessments
- Billing and payment information
- Insurance information
- Any other information created or received that relates to your past, present, or future physical or mental health

Use: Activities within our practice involving PHI, such as sharing, examining, utilizing, applying, or analyzing information.

Disclosure: Release, transfer, provision of access to, or divulging of PHI to persons or entities outside our practice.

Treatment: The provision, coordination, or management of health care and related services. This includes consultation between health care providers regarding your care and referrals for services.

Payment: Activities undertaken to obtain reimbursement for health care services, including billing, collections, claims management, and determining eligibility and coverage.
Health Care Operations: Administrative, financial, legal, and quality improvement activities that are necessary to run our practice and ensure quality care.
Minimum Necessary: The principle that we will make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose.
Business Associate: A person or entity that performs certain functions or activities on our behalf that involve the use or disclosure of PHI (examples: billing companies, EHR vendors, legal consultants).

---

3. HOW WE MAY USE AND SHARE YOUR HEALTH INFORMATION

The following section describes different ways we may use and disclose your protected health information. Not every use or disclosure will be listed. However, all of the permitted uses and disclosures will fall into one of these categories.

3.1 Treatment

We may use and disclose your PHI to provide, coordinate, or manage your mental health care and related services. This includes coordination or management of your care with other health care providers.

Examples of treatment uses and disclosures:

- **Consultation with other providers:** We may disclose information to your psychiatrist, primary care physician, or other mental health professionals involved in your care, with your consent
- **Coordination of services:** We may share information with case managers, care coordinators, or other professionals helping to manage your treatment
- **Emergency situations:** If you need emergency treatment, we may disclose information to emergency responders or emergency room staff
- **Referrals:** When referring you to another provider, we may share relevant treatment information
- **Continuity of care:** If treatment is transferred to another provider, we may share your treatment history

Our approach to collaborative care: We believe in collaborative treatment when appropriate and will discuss with you before consulting with other providers. You have the right to request restrictions on these disclosures.

3.2 Payment

We may use and disclose your PHI to bill and collect payment for the treatment and services we provide to you.

Examples of payment uses and disclosures:

- **Billing activities:** Creating and submitting bills and claims to you, your insurance company, or other payers

- **Claims management:** Processing and responding to requests for additional information from insurance companies
- **Payment collection:** Collecting payment from you, your insurance company, or third parties
- **Determining coverage:** Verifying your insurance coverage and benefits
- **Pre-authorization:** Obtaining approval for services from your insurance company
- **Utilization review:** Responding to insurance company reviews of medical necessity
- **Coordination of benefits:** Working with multiple insurance companies when you have more than one policy

Important information about insurance billing:
When we submit claims to your insurance company, we must include:

- Your name and identifying information
- Dates of service
- Type of service provided (procedure codes)
- Diagnosis codes
- Provider information
- Sometimes treatment notes or summaries if requested by the insurance company

Insurance records are permanent: Once we submit information to your insurance company, it becomes part of your permanent insurance record. Your insurance company may share this information with:

- The Medical Information Bureau (MIB)
- Other insurance companies
- Employers (in limited circumstances for self-funded plans)
- Government agencies for oversight and auditing

You have options:

- You may choose to pay out-of-pocket and not use insurance
- If you pay in full for a service out-of-pocket, you can request that we not submit that service to your insurance, and we will honor that request
- You may request restrictions on what we disclose to your insurance company, though we are not required to agree except in the situation mentioned above

3.3 Health Care Operations
We may use and disclose your PHI for our health care operations, which are activities necessary to run our practice and ensure that quality care is delivered.
Examples of health care operations:

- **Quality improvement:** Reviewing and analyzing treatment outcomes to improve our services
- **Training and supervision:** Training students, interns, or other providers (with PHI limited to what is necessary)
- **Compliance activities:** Ensuring compliance with professional standards and legal requirements
- **Business planning:** Analyzing practice operations for strategic planning

- **Credentialing and accreditation:** Participating in credentialing activities with insurance companies or professional organizations
- **Legal and administrative services:** Consulting with attorneys, accountants, or other professional advisors
- **Customer service:** Responding to your questions and complaints
- **Audit and monitoring:** Conducting internal audits to ensure proper documentation and billing

Our commitment to your privacy in operations: Even for operational purposes, we follow the "minimum necessary" standard, meaning we limit the information used or disclosed to the minimum amount needed for the specific purpose.

3.4 Technology and Security Measures

We take the security of your information seriously and use multiple technologies and procedures to protect it:

Electronic Health Records System:

We use **Counsol**, a HIPAA-compliant electronic health records (EHR) system. This system includes:

- End-to-end encryption of all data
- Secure access controls (password protected, multi-factor authentication)
- Automatic data backups
- Audit logs tracking all access to your records
- Automatic session timeouts for security
- Regular security updates and patches

Telehealth Platform:

We offer secure video sessions through **Doxy.me**, which is:

- HIPAA-compliant and designed specifically for healthcare
- Encrypted end-to-end
- Does not require you to download software
- Does not record sessions without explicit permission
- Does not store session data

Client Portal:

Your secure client portal at **mosaicbloom.secure-client-area.com** provides:

- Encrypted messaging for sensitive communications
- Secure document upload and download
- Protected access to your billing and appointment information
- Two-factor authentication options

Communication Security:

- **Secure communications:** Client portal messaging for sensitive information
- **Standard email and text:** Appropriate for scheduling and general communication only
- **Phone:** Routine matters only, not for detailed clinical discussions
- **Fax:** 267-202-5448 - encrypted fax for receiving documents from other providers

Physical Security:

- Locked office when unoccupied
- Secure file storage
- Shredding of paper documents containing PHI
- Limited access to areas where PHI is stored

Business Associate Agreements:
We maintain Business Associate Agreements with all vendors who have access to PHI, including:

- Counsol (EHR system)
- Doxy.me (telehealth platform)
- Payment processor
- Billing services (if applicable)
- IT support services

---

4. WHEN WE MUST SHARE YOUR INFORMATION WITHOUT YOUR CONSENT
There are some situations when federal or state law requires or permits us to use or disclose your PHI without your consent or authorization. In these situations, we will disclose only the minimum amount of information necessary.

4.1 To Protect You or Others from Serious and Imminent Harm
When we believe there is a serious and imminent threat to your safety or the safety of others, we may disclose PHI to:

- Law enforcement officials
- Family members or others who can help
- Medical or emergency personnel
- The person(s) who may be in danger

Pennsylvania law requires us to take action when we have a reasonable belief that you:

- Are at imminent risk of suicide or self-harm
- Pose an imminent risk of harm to others
- Are unable to care for yourself and are in danger

Our clinical judgment: Determining when a threat rises to the level requiring disclosure is a clinical judgment. We take these decisions very seriously and will discuss safety planning with you whenever possible before making disclosures.

4.2 Child Abuse and Neglect Reporting
Pennsylvania law mandates that we report suspected child abuse to ChildLine and/or local authorities.
We are required to make a report when we have reasonable cause to suspect that:

- A child under 18 years of age is a victim of child abuse
- A child has come before us in our professional capacity and we have reasonable cause to suspect abuse

What we must report:

- Name, age, and address of the child
- Name and address of parent/guardian

- Nature and extent of injuries or abuse
- Any other information that may be helpful in establishing the cause of abuse

Reporting contacts:

- **ChildLine (statewide 24/7):** 1-800-932-0313
- **Montgomery County Children and Youth Services:** 610-278-3000

Confidentiality after reporting: The fact that a report was made is confidential under Pennsylvania law, and we may not disclose to you or others that a report was filed unless required by a court.

4.3 Adult and Vulnerable Adult Abuse

We are required to report suspected abuse, neglect, or exploitation of:

- Adults aged 18 and older who are unable to protect themselves due to physical or mental incapacity
- Residents of care facilities
- Older adults (60+) who may be victims of abuse or exploitation

Montgomery County Adult Protective Services: Part of Aging and Adult Services - 610-278-3601

4.4 Domestic Violence

Pennsylvania law permits (but does not always require) disclosure when we have reasonable cause to believe that an individual is a victim of domestic violence.

We may report to law enforcement when:

- There is an imminent threat of serious harm
- The victim consents to the report
- It is necessary to protect the victim or others

Montgomery County Domestic Violence Resources:

- **Laurel House:** 1-800-642-3150 (24/7 hotline)

4.5 Health Oversight Activities

We must provide information to state licensing boards and other health oversight agencies for activities authorized by law, such as:

Pennsylvania State Board of Social Workers, Marriage and Family Therapists and Professional Counselors:

- Investigations of complaints against licensed professionals
- Audits and inspections
- Disciplinary proceedings
- License verifications

Other oversight agencies:

- State insurance departments
- Medicaid/Medicare fraud units
- Office of Inspector General
- Other governmental agencies with legal authority

4.6 Judicial and Administrative Proceedings

We may disclose PHI in response to:

Court orders: We must comply with valid court orders requiring disclosure of your records

Subpoenas: We may disclose information in response to a subpoena when:

- You have authorized the disclosure
- We have made reasonable efforts to notify you of the subpoena and you have not objected
- A court has issued a qualifying protective order

Our practice: When we receive a subpoena, we will:

1. Notify you immediately (unless prohibited by law)
2. Seek your written authorization to release records
3. If you object, we will assist you in filing a motion to quash the subpoena
4. Only release information if legally required to do so

Depositions and testimony: If called to testify about your treatment:

- We will notify you and seek your consent
- We will limit testimony to only what is legally required
- We will charge our standard court appearance rate as outlined in the Therapy Agreement

4.7 Law Enforcement Purposes

We may disclose limited PHI to law enforcement in specific situations:

- In response to a court order, warrant, subpoena, or summons
- To identify or locate a suspect, fugitive, material witness, or missing person
- About a victim of a crime under limited circumstances
- About a death that may be the result of criminal conduct
- About criminal conduct at our office
- In an emergency to report a crime, location of the crime or victims, or the identity of the perpetrator

Our approach: We balance legal requirements with our commitment to your privacy and will disclose only the minimum information necessary.

4.8 Coroners, Medical Examiners, and Funeral Directors

We may disclose PHI to:

- Coroners or medical examiners for death investigations
- Funeral directors as necessary for them to carry out their duties

4.9 Military and Veterans

If you are a member of the armed forces, we may disclose PHI as required by military command authorities.

4.10 Workers' Compensation

If you file a workers' compensation claim, we are required to provide relevant records to:

- Your employer's workers' compensation insurance carrier
- The workers' compensation board or commission
- Your attorney or your employer's attorney

Scope of disclosure: We will disclose only information relevant to the workers' compensation claim.

4.11 National Security and Intelligence Activities

We may disclose PHI to authorized federal officials for:

- Intelligence and counterintelligence activities
- Protection of the President or other authorized persons
- National security activities authorized by law

4.12 Inmates and Correctional Institutions

If you are an inmate of a correctional institution or under the custody of law enforcement, we may disclose PHI to the institution or law enforcement when necessary for:

- Your health and safety
- The health and safety of other inmates
- The health and safety of officers and employees of the correctional institution
- Law enforcement on the premises
- Administration and maintenance of the safety and security of the correctional institution

4.13 Public Health Activities

We may disclose PHI for public health activities, including:

- Preventing or controlling disease, injury, or disability
- Reporting births and deaths
- Reporting child abuse or neglect
- Reporting reactions to medications or problems with products
- Notifying people of recalls of products they may be using
- Notifying a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease

4.14 Research

Under certain limited circumstances, we may use or disclose your PHI for research purposes. However, we will only do so when:

- An institutional review board or privacy board has reviewed the research and established protocols to ensure privacy
- We obtain your written authorization
- The research occurs after your death
- The research involves only a limited data set with certain identifiers removed

---

5. WHEN WE NEED YOUR WRITTEN AUTHORIZATION

For most uses and disclosures not described in the sections above, we need your written authorization. Here are the main situations requiring your permission:

5.1 Sharing Information with Family, Friends, and Others
We need your written authorization before we can:

- Discuss your treatment with family members, friends, or significant others
- Share information with your employer
- Share information with schools or educational institutions
- Share information with attorneys (yours or others)
- Share information with other healthcare providers not involved in your treatment
- Share information with clergy or spiritual advisors

Exception: In emergency situations or when you are unable to communicate, we may share information with family members or others if we determine it is in your best interest.

5.2 Marketing
We will never use or disclose your PHI for marketing purposes without your written authorization.
Marketing means communication that encourages you to purchase or use a product or service.
What is NOT considered marketing:

- Communications about your treatment, case management, or care coordination
- Recommendations for alternative treatments, therapies, providers, or care settings

5.3 Sale of Information
We will never sell your PHI. This means we will not receive any form of direct or indirect compensation in exchange for your PHI without your written authorization.
Exception: We may receive reasonable, cost-based fees for:

- Copying and mailing your records
- Creating a summary or explanation of your PHI

5.4 Psychotherapy Notes
Most disclosures of psychotherapy notes require your specific written authorization. See Section 9 for detailed information about psychotherapy notes.

5.5 Uses and Disclosures Not Described in This Notice
Any other uses or disclosures not described in this notice will only be made with your written authorization.

5.6 Revoking Your Authorization
You have the right to revoke any authorization you give us at any time by submitting a written revocation.
Important: Revocation is not effective for:

- Actions we have already taken in reliance on your authorization

- Uses and disclosures that are required or permitted by law without your authorization

How to revoke: Send written notice to: Marquita Bolden, LCSW 8302 Old York Road, Suite B1 Elkins Park, PA 19027

---

6. YOUR PRIVACY RIGHTS - DETAILED EXPLANATION

You have the following rights regarding your protected health information:

6.1 Right to Inspect and Copy Your Health Information

You have the right to inspect and obtain a copy of your PHI that may be used to make decisions about your care, including:

- Medical and billing records
- Progress notes and treatment plans
- Assessment and evaluation reports
- Correspondence related to your treatment

How to request access:

Submit a written request to: Marquita Bolden, LCSW 8302 Old York Road, Suite B1 Elkins Park, PA 19027

Or via email: mbolden@mosaicbloomcounseling.com

Or through the secure client portal: https://mosaicbloom.secure-client-area.com

Our response timeline:

We will respond to your request within **30 days**. If we need more time, we may extend the response period by up to 30 additional days, but we will notify you of the delay and the reason.

Fees:

We may charge a reasonable, cost-based fee for:

- Copying your records
- Postage (if you request mailing)
- Preparing a summary or explanation (if you request this instead of copies)

Current fees (subject to Pennsylvania law limits):

- Paper copies: $0.64 per page
- Electronic copies: Minimal fee for media (USB drive, CD)
- Mailing costs: Actual postage charges

Denials:

We may deny your request in certain limited circumstances:

- Psychotherapy notes (which are kept separately from your medical record)
- Information compiled for legal proceedings
- Information about another person (unless that person is a health care provider)
- Information created or obtained in the course of research that includes treatment (while the research is in progress and you agreed to temporary denial)

If we deny your request:

- We will provide a written denial explaining the reason
- We will describe your right to have the denial reviewed (if applicable)
- We will provide information about how to file a complaint

Reviewable denials: For certain denials, you have the right to have the denial reviewed by a licensed healthcare professional who was not involved in the original denial. We will comply with the outcome of the review.

6.2 Right to Request an Amendment

If you believe that information in your record is incorrect or incomplete, you have the right to request that we amend it.

How to request an amendment:

Submit a written request that:

- Identifies the information you want amended
- Explains why you believe the information is incorrect or incomplete
- Suggests the correct or complete information

Send to: Marquita Bolden, LCSW 8302 Old York Road, Suite B1 Elkins Park, PA 19027

Our response:

We will respond within **60 days**. If we need more time, we may extend by up to 30 additional days with written notice.

We may approve or deny your request:

If we approve:

- We will make the amendment
- We will inform you that the amendment was made
- We will tell you how we will notify others of the amendment
- We will ask you to identify others who should be notified

If we deny:

- We will provide a written denial explaining the reason
- You may submit a statement of disagreement (which we will include with your record)
- We may prepare a rebuttal to your statement of disagreement
- We will attach your request, our denial, your statement, and our rebuttal (if any) to your record

Reasons we may deny your request:

- The information was not created by us (unless the person who created it is no longer available)
- The information is not part of the records we maintain
- The information is not part of the records you would be permitted to inspect
- The information is accurate and complete

6.3 Right to an Accounting of Disclosures

You have the right to receive a list (accounting) of certain disclosures we have made of your PHI.

What's included in the accounting:

Disclosures made:

- To public health agencies
- In response to law enforcement requests

- For health oversight activities
- In response to court orders
- For workers' compensation
- To coroners or medical examiners
- For other purposes required or permitted by law

What's NOT included:

- Disclosures for treatment, payment, or health care operations
- Disclosures made to you
- Disclosures you authorized
- Disclosures to family members or friends involved in your care
- Disclosures for national security purposes
- Disclosures to correctional institutions (in some cases)
- Disclosures made prior to the compliance date of the HIPAA Privacy Rule

Time period:

You may request an accounting for up to the **past 6 years** (but not for disclosures made before April 14, 2003).

How to request:

Submit a written request specifying the time period desired.

Our response:

We will provide the accounting within **60 days**, unless we notify you that we need an additional 30 days.

Fees:

- The first accounting in any 12-month period is **free**
- We may charge a reasonable fee for additional requests during the same 12-month period
- We will notify you of the fee and give you the opportunity to withdraw or modify your request

What the accounting will include:

For each disclosure:

- Date of the disclosure
- Name and address (if known) of the person or entity who received the information
- Brief description of the information disclosed
- Brief statement of the purpose of the disclosure

6.4 Right to Request Restrictions

You have the right to request restrictions on how we use or disclose your PHI for treatment, payment, or health care operations. You also have the right to request restrictions on disclosures to family members or others involved in your care.

How to request a restriction:

Submit a written request that:

- Identifies what information you want to limit
- Specifies whether you want to limit our use, disclosure, or both

- Identifies to whom you want the restriction to apply

We are NOT required to agree to your requested restriction, except in one specific situation (see below).

If we agree:

- We will document the restriction
- We will comply with your request except in emergency situations
- The restriction applies until you revoke it or we notify you that we are terminating the agreement

Exception - We MUST agree in this situation:

If you pay out-of-pocket in full for a service and request that we not disclose information about that service to your health plan, **we must agree** to your request (unless we are otherwise required by law to make the disclosure).

This means:

- Pay in full at time of service
- Specify that you do not want the service billed to insurance
- We will not submit a claim for that service
- We will not disclose information about that service to your insurance company

How to revoke a restriction:

You may revoke a restriction at any time by submitting a written request. The revocation will not apply to information already disclosed in reliance on the restriction.

6.5 Right to Request Confidential Communications

You have the right to request that we communicate with you about your PHI in a certain way or at a certain location.

Examples:

- Contact you only at work instead of home
- Send mail to a P.O. Box instead of your home address
- Call only your cell phone, never your home phone
- Use only secure portal messages, no phone calls
- Send communications in a sealed envelope without our practice name on it

How to request:

Submit a written or verbal request specifying:

- How you want to be contacted
- Where you want to be contacted

We will accommodate reasonable requests without asking for an explanation of why you are making the request.

Verbal requests: While we prefer written requests, we will honor verbal requests for confidential communications in emergency situations.

6.6 Right to a Paper Copy of This Notice

You have the right to a paper copy of this Notice of Privacy Practices at any time, even if you have agreed to receive it electronically.

How to request:

- Ask during any appointment
- Call 267-227-0122
- Email mbolden@mosaicbloomcounseling.com
- Download from www.mosaicbloomcounseling.com

We will provide a paper copy promptly.

6.7 Right to Be Notified of a Breach

You have the right to be notified if there is a breach of your unsecured PHI. See Section 12 for details about breach notification.

6.8 Right to Choose Someone to Act for You (Personal Representative)

You have the right to designate someone to act on your behalf regarding your health information. See Section 19 for detailed information about personal representatives.

---

7. YOUR CHOICES ABOUT HOW WE SHARE YOUR INFORMATION

In some situations, you can tell us your preferences about how we share your information. In these cases, we will follow your instructions.

7.1 Sharing with Family, Friends, and Others Involved in Your Care

You can tell us to:

- Share information with specific family members or friends
- Not share information with specific people
- Share only certain types of information

How we may share when you give permission:

- Discussing your treatment with family members
- Providing updates on your condition
- Coordinating care with others helping you
- Billing or payment matters

Your control: You can change your mind about these preferences at any time.

7.2 Disaster Relief Situations

In a disaster, you can tell us whether to share information with disaster relief organizations (such as the Red Cross) that are authorized by law to receive information to help notify family and friends about your location and condition.

7.3 When You Are Unable to Tell Us Your Preferences

If you are unable to tell us your preferences (for example, if you are unconscious or in an emergency):

- We may share information if we believe it is in your best interest
- We will use our professional judgment to determine what is best for you

- We will share only information that is directly relevant to the person's involvement in your care

After the emergency: Once you are able to communicate again, we will ask for your preferences going forward.

---

8. MULTI-STATE PRACTICE CONSIDERATIONS

Mosaic Bloom Counseling is licensed to provide services in multiple states, which creates some unique privacy considerations.

8.1 Jurisdictions Where We Are Licensed

We are currently licensed in:

- **Pennsylvania** - License CW016920
- **Delaware** - License Q1-0012314
- **New Jersey** - License 44SC06360400
- **Idaho** - License LCSW-43794

8.2 Applicable Privacy Laws

Your PHI is protected under:

- **Federal law:** Health Insurance Portability and Accountability Act (HIPAA)
- **State laws:** Privacy laws in each state where we are licensed
- **Professional standards:** Ethical codes of the National Association of Social Workers and state licensing boards

When state law is more protective: When state law provides greater privacy protections than federal HIPAA regulations, we will follow the more protective state law.

Examples of state-specific protections:

- Some states have stricter rules about disclosing mental health information
- Some states have different requirements for minor consent and parental access
- Some states have specific laws about HIV/AIDS information
- Some states have additional protections for substance abuse treatment records

8.3 Telehealth Across State Lines

When you receive telehealth services from us:

You must be physically located in one of our licensed states at the time of the session:

- Pennsylvania
- Delaware
- New Jersey
- Idaho

You must inform us if you will be in a different location than usual for a telehealth session, including:

- If you are traveling to a different state

- If you have moved to a new state
- If you are temporarily staying somewhere else

We will document your location for each telehealth session for licensing and legal compliance.

Interstate practice rules: Providing services across state lines requires that:

- We are licensed in the state where you are located
- We follow the laws of the state where you are located
- We may need to follow laws of multiple states if different from our home state

Important: We cannot provide telehealth services if you are located in a state where we are not licensed.

8.4 Mandatory Reporting Varies by State

Reporting requirements for child abuse, adult abuse, and duty to warn situations may vary by state. We will follow the requirements of the state where you are located at the time of service.

8.5 Records Retention

We maintain records according to the longest retention period required among all jurisdictions where we practice. Currently, we retain:

- Adult records: 7 years after last date of service
- Minor records: Until age 25 or 7 years after last service, whichever is longer

---

9. PSYCHOTHERAPY NOTES AND SPECIAL PROTECTIONS

Psychotherapy notes have special privacy protections that are different from your general medical record.

9.1 What Are Psychotherapy Notes?

Psychotherapy notes (also called "process notes" or "personal notes") are notes recorded by a mental health professional that:

- Document or analyze the contents of conversation during a private counseling session
- Are kept separate from the rest of your medical record
- Are used by the therapist for personal clinical use

Psychotherapy notes include:

- The therapist's analysis of the session
- Impressions and theories about your treatment
- Personal observations about therapy process
- Therapeutic hypotheses and formulations
- Content of conversations beyond what's documented in the medical record

Psychotherapy notes do NOT include:

- Medication prescription and monitoring
- Counseling session start and stop times
- Modalities and frequencies of treatment
- Results of clinical tests

- Diagnoses
- Functional status
- Treatment plans
- Symptoms
- Prognosis
- Progress to date

These items are part of your regular medical record (called your "designated record set") and may be used for treatment, payment, and health care operations.

9.2 Special Protections

Most uses and disclosures of psychotherapy notes require your specific written authorization.

This means:

- Even if you sign a general release of medical records, psychotherapy notes cannot be released without a separate specific authorization
- Insurance companies cannot require release of psychotherapy notes as a condition of payment
- We cannot release psychotherapy notes to others without your explicit permission

9.3 Exceptions - When We Can Use Psychotherapy Notes Without Your Authorization

We may use psychotherapy notes without your authorization only for:

1. **Our own training and supervision:**
    - Training of students and interns
    - Clinical supervision
    - Consultation with colleagues for educational purposes
2. **Our own defense:**
    - Defending ourselves in legal proceedings brought by you
    - Defending against professional liability claims
3. **When required by law:**
    - To health oversight agencies investigating our practice
    - To coroner or medical examiner for death investigations
    - To avert a serious and imminent threat to health or safety

9.4 Your Access to Psychotherapy Notes

You do NOT have a right to access psychotherapy notes under HIPAA. However:

- We may choose to allow you to review them if clinically appropriate
- Some state laws may provide additional access rights
- You always have the right to access your regular medical record

9.5 Our Practice Regarding Psychotherapy Notes

Transparency: We will discuss with you at the beginning of treatment:

- Whether we keep psychotherapy notes
- How they are different from your regular record
- Why they may benefit your treatment

Your choice: If you are uncomfortable with us keeping psychotherapy notes, please discuss this with us. While they can be clinically beneficial, we can modify our approach if you prefer.

---

10. PRIVACY PROTECTION AFTER DEATH

Your privacy rights continue after your death.

10.1 Duration of Protection

Under HIPAA, your health information remains protected for **50 years following your death**.

10.2 Who Can Exercise Your Rights

After your death, the following individuals may exercise your privacy rights:

Personal representatives of your estate:

- Executor or administrator of your will
- Person appointed by a court to administer your estate

Family members or others involved in your care or payment for care before your death (unless you previously expressed a preference that such persons not have access)

10.3 What We May Disclose

After your death, we may disclose your health information to:

Personal representatives: As necessary to carry out their duties

Family members and others: Who were involved in your care or payment for care before your death, unless you had previously directed us not to disclose information to them

Funeral directors and coroners: As necessary to carry out their duties

Organ procurement organizations: For purposes of facilitating organ, eye, or tissue donation

Law enforcement: In the case of suspicious death or death investigation

Public health authorities: For vital statistics and other public health purposes

10.4 Honoring Your Wishes

If you documented preferences during your life about information disclosure after death (such as in an advance directive or through a specific written request to us), we will honor those preferences to the extent possible under law.

---

11. MARKETING AND SALE OF INFORMATION

We take seriously our obligation not to exploit your health information for commercial purposes.

11.1 Marketing

We will NEVER use or disclose your PHI for marketing purposes without your written authorization.

What is marketing?

Marketing means a communication that encourages you to purchase or use a product or service.

Examples of marketing:

- Encouraging you to purchase a particular wellness program
- Promoting a product or service we would benefit from financially
- Sending information about non-health-related products or services

What is NOT marketing (and doesn't require authorization):

Communications about:

- Your treatment, case management, or care coordination
- Alternative treatments, therapies, providers, or settings
- Health-related products or services we provide
- Appointment reminders
- Treatment alternatives
- Other health-related benefits and services

Our practice: We do not engage in marketing activities. Any communications you receive from us are about your treatment or our services.

11.2 Sale of Protected Health Information

We will NEVER sell your PHI.

This means we will not receive any form of direct or indirect remuneration (payment, compensation, benefit) in exchange for your PHI without your written authorization.

What is NOT considered a "sale":

- Providing copies of your records for reasonable, cost-based fees
- Treatment and payment purposes
- Required disclosures to public health authorities
- Research purposes (when approved by an institutional review board)
- Business associate agreements for services to our practice

11.3 Fundraising

We do not engage in fundraising activities, so your information will never be used for fundraising purposes.

---

12. BREACH NOTIFICATION PROCEDURES

Federal law requires us to notify you if there is a breach of your unsecured protected health information.

12.1 What Is a Breach?

A **breach** is an unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of your information.

Examples of potential breaches:

- Lost or stolen laptop, phone, or portable device containing your information
- Unauthorized employee access to your records
- Mailing information to wrong person
- Improper disposal of records
- Hacking or cyber security incident
- Accidental disclosure to unauthorized person

12.2 When We Will Notify You

Timeline: We will notify you **without unreasonable delay** and in no case later than **60 days** after we discover the breach.

Exceptions: We may delay notification if a law enforcement official determines that notification would impede a criminal investigation or damage national security.

12.3 How We Will Notify You

Method of notification:

First-class mail to your last known address, OR

Email if you have agreed to receive electronic communications from us and you have provided an email address, OR

Telephone if we cannot reach you by mail and we have your phone number

If we cannot reach you: We will post a notice on our website or in major media outlets if the breach affected more than 10 people and we have insufficient contact information.

12.4 What the Notification Will Include

The breach notification will provide:

Description of the breach:

- What happened
- When it happened
- When we discovered it

Types of information involved:

- What categories of PHI were affected
- How many individuals were affected

Steps you should take:

- Actions you can take to protect yourself from potential harm
- Resources available to you (such as credit monitoring if financial information was involved)

What we are doing:

- Steps we have taken to investigate
- What we are doing to prevent future breaches
- Who to contact for more information

Your rights:

- How to file a complaint

- Where to get more information

12.5 Breaches Affecting Large Numbers
If a breach affects **500 or more individuals** in a state or jurisdiction:
We will also notify:

- Prominent media outlets in the affected area
- The Secretary of Health and Human Services
- Post information on our website

12.6 Our Commitment to Prevention
We take the security of your information very seriously. We maintain comprehensive security measures including:
Administrative safeguards:

- Privacy and security policies and procedures
- Workforce training on HIPAA and security
- Regular risk assessments
- Incident response procedures
- Business associate oversight

Physical safeguards:

- Secure office facility
- Locked file storage
- Controlled access to areas containing PHI
- Proper disposal procedures (shredding)
- Device security measures

Technical safeguards:

- Encryption of electronic PHI
- Secure passwords and authentication
- Automatic logoff procedures
- Audit controls and monitoring
- Regular software updates and patches
- Firewall and antivirus protection
- Secure backup procedures

Ongoing monitoring:

- Regular security assessments
- Monitoring for unauthorized access
- Investigation of security incidents
- Updates to security measures as threats evolve

---

13. OUR RESPONSIBILITIES UNDER LAW
We are required by law to:

13.1 Maintain Privacy and Security

- Maintain the privacy and security of your protected health information
- Implement appropriate administrative, physical, and technical safeguards
- Ensure that our business associates protect your information
- Have workforce members sign confidentiality agreements
- Provide training to workforce members on privacy and security

13.2 Provide This Notice

- Provide you with this notice of our privacy practices
- Make this notice available on our website
- Post this notice in our office
- Provide a paper copy upon request

13.3 Follow This Notice

- Follow the terms of the notice currently in effect
- Not retaliate against you for filing a complaint or exercising your rights
- Not require you to waive your rights as a condition of treatment

13.4 Maintain Records

- Maintain records in accordance with applicable laws
- Protect records from unauthorized access or destruction
- Retain records for required time periods:
    - Adult clients: Minimum 7 years after last service
    - Minor clients: Until age 25 or 7 years after last service, whichever is longer

13.5 Report Breaches

- Investigate suspected breaches
- Notify affected individuals of breaches as required
- Report breaches to HHS as required
- Maintain documentation of breach assessments

13.6 Cooperate with Oversight

- Cooperate with Office for Civil Rights investigations
- Make records available to OCR as required
- Respond to complaints and investigations

13.7 Minimum Necessary Standard

- Make reasonable efforts to limit PHI used, disclosed, or requested to the minimum necessary to accomplish the intended purpose
- Implement policies to ensure minimum necessary disclosures
- Review practices periodically to ensure compliance

13.8 Use and Disclose Only as Permitted

- Not use or disclose your PHI other than as described in this notice unless you authorize us in writing
- Honor your authorization requests where required by law
- Track disclosures that must be included in an accounting of disclosures

---

14. CHANGES TO THIS PRIVACY NOTICE

14.1 Our Right to Change This Notice

We reserve the right to change the terms of this notice at any time. Changes will apply to all PHI we maintain, including information created or received before the change.

Why we might change this notice:

- Changes in federal or state law
- Changes in our practice operations
- Changes in technology
- Changes required by insurance companies or business associates
- To better protect your privacy

14.2 How We Will Notify You of Changes

When we make material changes to this notice:

We will:

- Post the revised notice in our office waiting area
- Post the revised notice on our website at www.mosaicbloomcounseling.com
- Make copies available through the client portal
- Provide you with a copy at your next appointment if the change is substantial

The notice will always display:

- The effective date on the first page
- A version number
- Date of most recent revision

14.3 How to Get the Current Notice

You may request a copy of the current notice at any time:

- During any appointment (ask and we'll provide a copy)
- By phone: 267-227-0122
- By email: mbolden@mosaicbloomcounseling.com
- Download from website: www.mosaicbloomcounseling.com
- Through client portal: https://mosaicbloom.secure-client-area.com

We will provide a paper copy promptly at no charge.

---

15. DIGITAL COMMUNICATIONS AND TECHNOLOGY SECURITY

15.1 Types of Digital Communication

We use various forms of digital communication, each with different levels of security:

Most Secure - Client Portal:

- mosaicbloom.secure-client-area.com
- HIPAA-compliant encrypted messaging
- Secure document upload/download
- Best for: Sensitive clinical discussions, sharing documents, detailed questions

Moderately Secure - Email:

- Standard email (Gmail) is NOT encrypted
- Appropriate for: Scheduling, general questions, administrative matters
- NOT appropriate for: Detailed clinical information, sensitive personal information
- If you email sensitive information, we will respond via the secure portal

Least Secure - Text Message:

- SMS text messages are NOT encrypted
- Appropriate for: Appointment reminders, quick scheduling questions
- NOT appropriate for: Any clinical information, personal details

Telehealth - Doxy.me:

- HIPAA-compliant video platform
- Encrypted end-to-end
- Only for scheduled therapy sessions
- Cannot be recorded without explicit permission

15.2 Your Responsibilities for Digital Security

To protect your privacy when using digital communications:

For Telehealth Sessions:

- Use a private location where you won't be overheard
- Use secure internet (not public WiFi)
- Close doors and windows
- Use headphones if others are nearby
- Ensure no one can see your screen
- Don't record sessions without explicit permission

For Email and Text:

- Use a personal device/account that others don't access
- Use strong passwords
- Enable two-factor authentication when available
- Be cautious about what information you include
- Don't forward emails containing PHI without deleting previous content

For Client Portal:

- Don't share your login credentials
- Log out when finished
- Use a strong, unique password

- Don't access from public computers
- Enable two-factor authentication if offered

15.3 Email and Text Message Policy

What we will do:

- Respond to scheduling and administrative questions
- Send appointment reminders
- Send general practice information
- Request that you use the secure portal for sensitive matters

What we will NOT do:

- Discuss detailed clinical information via email or text
- Send you clinical documents via standard email
- Engage in therapy via text message
- Send sensitive information without encryption

If you email us sensitive information:

- We will acknowledge receipt
- We will respond through the secure portal
- We will not continue sensitive discussions via standard email

15.4 Emergency Situations

Email and text are NOT monitored for emergencies.

If you are experiencing a mental health emergency:

- Call 911
- Go to nearest emergency room
- Call National Suicide Prevention Lifeline: 988 or 1-800-273-8255
- Text HOME to 741741 (Crisis Text Line)
- Call Montgomery County Emergency Services: 610-279-6100

For urgent (non-emergency) matters: Call our office at 267-227-0122

15.5 Technology Changes

As technology evolves, we may:

- Add new secure communication methods
- Update our security measures
- Change platforms or systems
- We will notify you of any significant changes that affect how you communicate with us

---

16. INSURANCE AND PAYMENT INFORMATION DISCLOSURE

This section provides detailed information about what happens when you use insurance for mental health services.

16.1 What Information Insurance Companies Require

When you use insurance, we must submit claims that include:

Basic identifying information:

- Your name, date of birth, address
- Insurance ID number
- Our provider information (name, NPI, tax ID)

Service information:

- Date(s) of service
- Type of service (procedure code - CPT code)
- Length of session
- Location of service (office vs. telehealth)

Diagnostic information:

- Mental health diagnosis code(s) (ICD-10 codes)
- Sometimes additional codes for other conditions affecting treatment

Sometimes additional information:

- Treatment plans
- Progress notes or session summaries
- Assessment reports
- Medical necessity documentation
- Treatment authorization requests

16.2 What Happens to This Information

Once submitted to your insurance company, this information:

Becomes part of your permanent insurance record which may include:

- Insurance company's claims database
- Medical Information Bureau (MIB) - a consortium of insurance companies that share medical information
- Other insurance companies (if you apply for new coverage)
- Employers (in limited circumstances for self-funded plans)

May be used for:

- Processing your claims
- Determining eligibility and coverage
- Utilization review
- Quality assurance activities
- Fraud detection
- Underwriting for future insurance coverage (in some states)
- Research and data analysis (de-identified)

Cannot be used for:

- Employment decisions (with limited exceptions)
- Most housing decisions (with limited exceptions)
- Protected by various federal and state anti-discrimination laws

16.3 Your Insurance Company's Rights

Your insurance company may:

Review your records:

- Request progress notes
- Request treatment plans
- Request assessment reports
- Conduct audits of our documentation

Require pre-authorization for:

- Initial treatment
- Continued treatment beyond certain number of sessions
- Specific types of services

Deny coverage if:

- Services are not medically necessary
- Services are not covered under your plan
- Pre-authorization was not obtained
- Documentation doesn't support medical necessity

16.4 Our Current Insurance Participation

We are currently in-network with:

- **Aetna** (various plans)

What "in-network" means:

- We have a contract with the insurance company
- We accept the insurance company's allowed amount as payment in full
- You typically pay only your copay, coinsurance, or deductible
- We bill the insurance company directly
- The insurance company pays us directly

Out-of-network insurance: For all other insurance companies, we are considered out-of-network, which means:

- You may have out-of-network benefits
- You typically pay us at time of service
- We provide you with a "superbill" to submit to your insurance
- Your insurance may reimburse you directly (partial reimbursement)
- Out-of-network deductibles and copays are typically higher

16.5 Your Options to Limit Insurance Company Access

Option 1: Pay Out-of-Pocket

- Pay for services yourself without using insurance
- Information stays completely private (except for situations requiring disclosure by law)
- No diagnosis goes to insurance company
- No claims or treatment information submitted

Option 2: Pay Out-of-Pocket for Specific Services

- Use insurance for some sessions
- Pay out-of-pocket for others
- We must agree not to submit claims for the self-pay sessions

- This can protect specific information while still using insurance benefits

Option 3: Request Restrictions on Disclosures

- Request that we not disclose certain information to your insurance company
- We are not required to agree (except for the self-pay situation above)
- Insurance company may deny coverage if we don't provide requested information

Important consideration: Many insurance plans have "coordination of benefits" clauses requiring you to report all health care services and providers. Paying out-of-pocket while having insurance coverage may violate your insurance contract in some cases.

16.6 Understanding Medical Necessity

What is "medical necessity"?

Medical necessity generally means:

- Services are appropriate for your diagnosis
- Services are expected to improve your condition
- Services are not primarily for convenience
- Services meet generally accepted standards of care

Why it matters:

Insurance companies only cover "medically necessary" services. This means:

- The diagnosis must meet criteria for treatment
- The treatment must be appropriate for the diagnosis
- Progress toward goals must be documented
- Continued treatment must show ongoing benefit

Our role:

- We document medical necessity in our treatment plans and progress notes
- We respond to insurance company requests for information
- We advocate for coverage when we believe services are medically necessary
- We cannot guarantee that insurance will agree with our assessment

16.7 Insurance Audits and Reviews

Insurance companies may conduct:

Concurrent review:

- Review treatment as it's occurring
- Request progress updates
- Require re-authorization for continued treatment

Retrospective review:

- Review claims after services have been provided
- May request records
- May request refunds if they determine services weren't covered

Fraud investigation:

- Review if they suspect billing errors or fraud
- May request extensive documentation
- Required to cooperate with these reviews

Your rights during reviews:

- Be informed when your records are reviewed
- Appeal denials of coverage
- File complaints about unfair reviews

---

17. SOCIAL MEDIA AND PROFESSIONAL BOUNDARIES

17.1 Social Media Policy

To maintain professional boundaries and protect your confidentiality:

We do NOT:

- Accept friend requests or connections on personal social media (Facebook, Instagram, LinkedIn, Twitter/X, TikTok, etc.)
- Follow clients on social media
- Search for clients on social media
- Communicate with clients through social media messaging
- Monitor social media platforms for client communications
- Respond to social media posts, comments, or messages from clients

Why we maintain these boundaries:

- To protect your privacy and confidentiality
- To maintain appropriate therapeutic boundaries
- To avoid dual relationships
- To ensure equity among all clients
- To protect the therapeutic relationship

If you send us a friend request or message on social media:

- We will not respond through social media
- We may mention it in our next session to discuss appropriate communication channels
- This is not a rejection of you personally - it's a professional boundary we maintain with all clients

17.2 If We See Each Other in Public

Our approach:

- We will not acknowledge our professional relationship unless you initiate contact
- If you choose to acknowledge us, we will keep the interaction brief and professional
- We will not discuss your treatment or any confidential matters

Why this protects you:

- Others won't know you are our client
- You can choose whether or not to acknowledge us
- You control who knows about our professional relationship

After a public encounter:

- We may briefly mention it in our next session if it seems relevant
- We can discuss how you'd like us to handle future encounters

17.3 Online Reviews

You have the right to:

- Post reviews about your experience with our services
- Share your opinions on review sites (Google, Psychology Today, etc.)

Please protect your own privacy:

- Avoid sharing details about your treatment
- Avoid sharing your diagnosis or personal information
- Remember that online reviews are public
- Consider using initials instead of full name

We cannot:

- Respond to reviews in a way that would confirm you are a client
- Acknowledge the existence of a therapeutic relationship
- Publicly thank you or comment on your review in detail
- Ask you to post or remove a review

What we can do:

- Respond to reviews in general terms without confirming the reviewer is a client
- Report reviews that violate the review platform's policies
- Appreciate honest feedback privately if you share it with us directly

17.4 Online Presence and Search Results

What you may find about us online:

- Professional website: www.mosaicbloomcounseling.com
- Psychology Today profile
- State licensing board information
- Professional directory listings

What you will NOT find:

- Personal social media that discusses clients
- Blog posts that identify clients
- Photos or information about clients

If you search for us online:

- That's perfectly normal and we understand curiosity about your therapist
- You're welcome to discuss anything you find in our sessions
- If you have questions about our qualifications or approach, please ask directly

17.5 Your Online Activity

We respect your privacy:

- We do not search for clients online
- We do not monitor clients' social media
- We do not "check up on" clients between sessions

However:

- Information you share with us about your online activity may be clinically relevant

- If you're concerned about your online behavior or social media use, we can discuss it in therapy
- If you show us something on your phone or device during a session, we will maintain that confidence

---

18. MINOR CLIENTS AND PARENTAL ACCESS

Special privacy considerations apply when treating clients under age 18.

18.1 Pennsylvania Law Regarding Minors

Pennsylvania law provides:

Ages 14-17:

- May consent to their own mental health treatment
- Parents/guardians do not need to consent
- Minors have same privacy rights as adults in many situations

Ages under 14:

- Parent/guardian consent typically required
- Parents/guardians generally have access to treatment information

Exceptions (any age):

- Emancipated minors have full adult rights
- Mature minors (determined case-by-case) may have enhanced rights
- Emergency situations

18.2 Our Approach to Minor Confidentiality

Our philosophy:

- We believe therapy works best when minors feel safe sharing openly
- We balance the minor's need for privacy with parents' need to be informed
- We tailor our approach to each family's unique situation

At the beginning of treatment, we will discuss:

- What information will be shared with parents/guardians
- What information will remain confidential
- Under what circumstances confidentiality might be broken
- How to handle situations where the minor and parents disagree

General guidelines:

- We typically share themes and general progress with parents
- We protect details of conversations unless there are safety concerns
- We involve minors in decisions about what to share with parents when appropriate
- We may meet with parents separately to discuss concerns

18.3 When We Must Break Confidentiality with Minors

Even when a minor has privacy rights, we must disclose information when:

Safety concerns:

- Risk of suicide or self-harm

- Risk of harm to others
- Serious dangerous behavior

Abuse or neglect:

- Suspected child abuse
- Suspected neglect
- Exploitation

Legal requirements:

- Court orders
- Mandated reporting obligations

Parental rights situations:

- When parents have legal right to information
- When minor lacks capacity to consent
- When disclosure is necessary for treatment

18.4 Parental Access to Records

Parents/guardians may request access to:

- Treatment summaries
- Diagnosis information
- General progress updates
- Billing and payment information

We may limit parental access to:

- Detailed session notes that could harm the therapeutic relationship
- Information the minor disclosed with expectation of privacy
- Psychotherapy notes (which have special protections for all clients)

Our process:

- When parents request records, we will usually discuss with the minor first
- We will explain why the request is being made
- We will involve the minor in deciding what to share when appropriate
- We will advocate for the minor's best interests

18.5 Special Situations

Divorced or separated parents:

- Usually both parents have equal access unless court order states otherwise
- We need clear documentation of custody and decision-making authority
- We will follow court orders regarding information access
- We encourage parents to communicate with each other about treatment when possible

Guardians and other caregivers:

- Must provide documentation of legal authority
- May have different rights than biological parents
- We will clarify roles and decision-making at start of treatment

Foster care:

- May involve multiple parties with information access rights

- We will clarify who can consent, access information, and make decisions

---

19. PERSONAL REPRESENTATIVES

19.1 What Is a Personal Representative?

A personal representative is someone who has legal authority to make health care decisions on your behalf or to act for you in matters related to your health care.

Common types of personal representatives:

For adults:

- Health care power of attorney (HCPOA)
- Legal guardian appointed by court
- Executor or administrator of deceased person's estate
- Individual with durable power of attorney for health care

For minors (under 18):

- Parents (in most situations)
- Legal guardians
- Person with legal custody

For deceased individuals:

- Personal representative of the estate
- Executor or administrator

19.2 Rights of Personal Representatives

A personal representative generally has the same rights as the individual to:

- Access health information
- Request amendments to health records
- Receive an accounting of disclosures
- Request restrictions on uses and disclosures
- Request confidential communications
- File complaints

19.3 Documentation Required

Before we can recognize someone as your personal representative, we need:

For health care power of attorney:

- Copy of signed and witnessed HCPOA document
- Verification that the document is currently in effect
- Verification of identity of the person acting as representative

For legal guardianship:

- Copy of court order appointing guardian
- Documentation of scope of guardianship
- Verification of identity of guardian

For minor's parent/guardian:

- Usually birth certificate, custody order, or guardianship papers

- Photo ID of parent/guardian

19.4 When We May Not Treat Someone as a Personal Representative
We may decline to treat someone as your personal representative when:
Abuse, neglect, or endangerment:
- We have reasonable belief that you are subject to abuse, neglect, or endangerment by the person
- Treating them as personal representative would not be in your best interest

State law limitations:
- When state law limits the authority of the personal representative
- When you have specifically revoked their authority
- When the personal representative's authority has expired

Minor situations:
- When a minor has legally consented to care on their own
- When disclosing to a parent would endanger the minor
- When state law provides privacy rights to the minor independent of parents

We will document our reasons when we decline to treat someone as a personal representative.

19.5 Revoking Personal Representative Authority
You may revoke someone's authority to act as your personal representative by:
- Providing written notice to us
- Providing evidence of legal revocation (such as revocation of power of attorney)
- Court order limiting or terminating the representative's authority

Effect of revocation:
- We will no longer provide information to the former representative
- The revocation will not affect information already disclosed
- We will document the revocation in your file

---

20. QUESTIONS, COMPLAINTS, AND HOW TO CONTACT US

20.1 Questions About This Notice
If you have questions about this Notice of Privacy Practices or about how we handle your health information, please contact:
Marquita Bolden, LCSW
Mosaic Bloom Counseling, LLC
8302 Old York Road, Suite B1 Elkins Park, PA 19027
Phone: 267-227-0122
Email: mbolden@mosaicbloomcounseling.com
Website: www.mosaicbloomcounseling.com
Secure Client Portal: https://mosaicbloom.secure-client-area.com
Office Hours:

- Tuesday (virtual): 2 PM - 5 PM
- Wednesday (office): 10 AM - 8 PM
- Thursday (office): 10 AM - 7 PM
- Sunday (office, biweekly): 10 AM - 6 PM

20.2 Filing a Complaint with Us

If you believe your privacy rights have been violated, you may file a complaint with us.

How to file:

Submit a written complaint that includes:

- Your name and contact information
- Description of what happened
- When it happened
- What privacy right you believe was violated
- Any other relevant information

Send to:

Marquita Bolden, LCSW 8302 Old York Road, Suite B1 Elkins Park, PA 19027
Email: mbolden@mosaicbloomcounseling.com

What will happen:

- We will acknowledge receipt of your complaint within 5 business days
- We will investigate your complaint promptly and thoroughly
- We will respond to you in writing within 30 days
- We will explain what we found and what actions we are taking

You will not be retaliated against in any way for filing a complaint.

20.3 Filing a Complaint with the Federal Government

You also have the right to file a complaint with the U.S. Department of Health and Human Services.

Office for Civil Rights

U.S. Department of Health and Human Services
801 Market Street, Suite 9300 Philadelphia, PA 19107-3134
Phone: 1-800-368-1019
Fax: 202-619-3818
TDD: 1-800-537-7697 (for hearing impaired)
Email: ocrmail@hhs.gov
Online complaint portal: www.hhs.gov/ocr/privacy/hipaa/complaints
Complaint deadline: Complaints must generally be filed within 180 days of when you knew (or should have known) that the violation occurred. The Office for Civil Rights may extend this deadline for good cause.

What to include in your complaint:

- Your name and contact information
- Name and address of the entity you're complaining about (Mosaic Bloom Counseling)
- Description of what happened

- When it happened
- How you believe your health information privacy was violated

What will happen:

- OCR will review your complaint
- OCR may contact you for additional information
- OCR may investigate the entity you complained about
- OCR will notify you of the outcome
- OCR may take enforcement action if violations are found

20.4 You Will Not Be Retaliated Against

Federal law protects you from retaliation for filing a complaint or exercising your privacy rights.

We will NOT:

- Terminate your treatment
- Refuse to provide treatment
- Take any adverse action against you
- Require you to waive your right to file a complaint
- Intimidate or threaten you

Your rights are protected, and we respect your right to file a complaint if you believe your privacy has been violated.

20.5 Other Resources

Pennsylvania State Board:

State Board of Social Workers, Marriage and Family Therapists and Professional Counselors P.O. Box 2649 Harrisburg, PA 17105-2649 Phone: 717-783-1389 Website: www.dos.pa.gov/social-workers

National Association of Social Workers:

NASW Pennsylvania Chapter Phone: 717-232-4125 Website: www.nasw-pa.org

---

ACKNOWLEDGMENT

This Notice of Privacy Practices describes how Mosaic Bloom Counseling, LLC may use and disclose your protected health information, and how you can access this information.

This notice is effective as of October 12, 2025.

A shorter summary version of this notice is provided to all clients at intake and is available on our website. This extended version provides comprehensive information about all aspects of our privacy practices.

For questions or concerns: Contact Marquita Bolden, LCSW at 267-227-0122 or mbolden@mosaicbloomcounseling.com

---

Mosaic Bloom Counseling, LLC
Marquita Bolden, LCSW
8302 Old York Road, Suite B1 Elkins Park, PA 19027
267-227-0122
www.mosaicbloomcounseling.com

This is a comprehensive informational document provided for your reference. You will be asked to acknowledge receipt of privacy practices information during your intake process.
For the most current version of this notice, visit www.mosaicbloomcounseling.com

---

END OF NOTICE
Document Information:

- Effective Date: October 12, 2025
- Version: 2.0 (Extended/Comprehensive)
- Pages: Approximately 30 pages
- Format: Downloadable PDF
- Purpose: Complete detailed reference guide