



This Notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

1. Our Legal Duty

We are required by law to maintain the privacy and security of your protected health information ("PHI") and to provide you with this Notice explaining our privacy practices. We must abide by the terms of this Notice currently in effect, and we are required by law to notify you following a breach of your unsecured PHI (see Section 8). When we use the term "protected health information," it includes any information that relates to your health, treatment, or payment for healthcare services, and that could reasonably be used to identify you.

This Notice is **effective June 10, 2026** and supersedes (replaces) the version dated April 9, 2025.

2. Uses & Disclosures of Your Health Information

Treatment

We may use or disclose your PHI to coordinate and manage your healthcare. For example, information obtained by Dr. Bray or other members of your healthcare team will be recorded in your record and used to determine your plan of care. If we refer you to another provider, we may share your PHI as necessary for that provider's treatment decisions.

Payment

We are a self-pay practice: we do not participate with insurance plans, Medicare, or Medicaid, and we file no insurance claims. Disclosures for payment purposes are limited to direct billing to you through our payment processor, **Stripe**. Stripe receives **billing data only** (such as your name, payment method, and amount charged) — **never your medical information**. Your clinical records are kept separate from billing systems.

Healthcare Operations

We may use and disclose your PHI for internal operations such as quality improvement, staff performance evaluation, training, scheduling, patient communications, and ensuring compliance with regulations.

Appointment Reminders & Communications

With your **opt-in** consent, we may contact you with appointment reminders and practice communications (for example, automated reminders through Athena Health, the patient portal, email, phone, or text). You may change or withdraw your communication preferences at any time.

3. Uses Requiring Your Written Authorization

The following uses and disclosures of PHI will be made **only with your written authorization** (your signed permission), which you may revoke (cancel) in writing at any time:

- **Marketing.** We will not use or disclose your PHI for marketing purposes without your written authorization.
- **Sale of PHI.** We will never sell your PHI. Any disclosure that would constitute a sale of PHI requires your written authorization — and it is our policy not to make such disclosures at all.
- **Psychotherapy notes.** The Practice does not maintain separate psychotherapy notes. If such notes were ever created, most uses and disclosures would require your written authorization.
- **Any other use or disclosure not described in this Notice.**

4. Other Permitted or Required Disclosures

In certain situations, we are permitted or required by law to disclose your PHI without your authorization. Examples include:

- **Public health activities:** reporting communicable diseases, reactions to medications or problems with products, or notifying a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease.
- **Health oversight activities:** providing information to governmental agencies responsible for monitoring the healthcare system or ensuring compliance with government program standards.
- **Legal proceedings:** disclosing PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process, when certain criteria are met.
- **Law enforcement purposes:** disclosures requested by a law enforcement official in order to locate a suspect, fugitive, material witness, or missing person; or pertaining to victims of a crime.
- **Serious threat to health or safety:** using or disclosing PHI when necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and when such disclosure is made to someone able to prevent or reduce the threat.

- **Workers' compensation:** as authorized by, and to the extent necessary to comply with, workers' compensation laws (note: the Practice does not conduct workers'-compensation visits).
- **Coroners, medical examiners, and funeral directors:** as necessary to carry out their duties.
- **Organ and tissue donation:** to organizations that handle organ, eye, or tissue procurement or transplantation.
- **Military and national security:** as required for military command authorities, authorized national security and intelligence activities, or protective services.
- **Persons involved in your care:** we may share information relevant to a family member's or friend's involvement in your care or payment for your care, unless you object. You may designate a contact person or restrict these disclosures (see Section 8).

5. How We Store & Protect Your Health Information

Your primary electronic health records are securely created, stored, and managed within our Athena Health Electronic Health Record (EHR) system. We use encrypted, HIPAA-compliant systems for storing and transmitting PHI, with access controls and other technical safeguards in place. We believe you have a right to know which vendors touch your information and how:

Vendors operating under a Business Associate Agreement (BAA)

A BAA is a contract that legally requires a vendor handling PHI on our behalf to meet strict HIPAA privacy and security standards. We maintain BAAs with:

- **Athena Health** — our electronic health record (EHR) system, where your medical record lives.
- **Microsoft 365** — HIPAA-compliant email and Microsoft Teams secure messaging.
- **Google Workspace (HIPAA tier)** — including voicemail storage and HIPAA-protected Gemini for any AI assistance involving PHI. All AI-assisted content is reviewed and verified by Dr. Bray before it is used or sent.
- **doxy.me** — backup telehealth video platform.
- **Doximity** — secure fax and telehealth dialer.

Vendors that do not handle PHI (no BAA needed)

- **Stripe** — payment processing only. Stripe receives billing data, never medical information, so no BAA is required.
- **Twilio** (phone system) and **ElevenLabs** (conversational AI receptionist) — our phone layer is configured for **non-retention** (it does not store call content), the AI receptionist instructs callers not to share personal health details, and the AI identifies itself as an AI at the start of each call. Voicemails are stored under the Google Workspace BAA described above.

Text messaging

Texting is **opt-in only**. To prevent impersonation, we use a one-time passcode (OTP) plus a PIN that expires every 15 minutes to verify identity. For clinical content we offer Microsoft Teams as a secure messaging channel; please be aware that **standard SMS text messaging is not fully secure**.

6. Record Retention

We retain patient medical records, primarily stored within the Athena Health EHR, for a minimum of **7 years after the last date of service**. For minors, records are retained **until the patient reaches age 25 or for 7 years after the last date of service, whichever is longer**. After the applicable period, records may be securely destroyed or archived unless otherwise required by law or for ongoing patient care.

7. Minors

For patients under the age of 18, we comply with all state and federal laws regarding parental or guardian consent and access to records. Consistent with Florida law, **written** parental or guardian consent is required for treatment of minors and for the handling of their PHI. Florida law provides limited statutory exceptions under which a minor may consent to their own care (for example, emergency care and certain specific services defined by statute); where such an exception applies, we follow the corresponding confidentiality rules.

8. Your Rights Regarding Your Health Information

Under HIPAA, you have the following rights regarding your PHI:

- **Right to request restrictions.** You may ask us not to use or disclose certain parts of your PHI for treatment, payment, or healthcare operations, or to persons involved in your care. We are not required to agree to every request, but if we do agree, we will comply except in an emergency.
- **Right to restrict disclosures to a health plan for self-paid services.** You have the right to require that we not disclose PHI to a health plan for services you have paid for in full out of pocket. Because we file no insurance claims for any patient, **this protection applies automatically to every service we provide**.
- **Right to confidential communications.** You may request that we communicate with you about medical matters in a certain way or at a certain location (e.g., only by mail, phone, or email). We will make reasonable efforts to accommodate such requests.
- **Right to choose a contact person.** You may designate a family member, friend, or other person we may communicate with about your care — or tell us not to communicate with particular persons.

- **Right to inspect and copy.** You have the right to inspect and obtain a copy of your PHI in our designated record set. We may charge a reasonable fee for copying, mailing, or other expenses associated with your request, as allowed by law.
- **Right to request an amendment.** If you feel the PHI we have about you is incorrect or incomplete, you may request that we amend it. We are not required to change your information if we determine that it is accurate and complete, or if other legal grounds apply. If we deny your request, we will inform you in writing.
- **Right to an accounting of disclosures.** You have the right to receive a list of certain disclosures we have made of your PHI in the past six years (excluding disclosures you authorized and those made for treatment, payment, or healthcare operations).
- **Right to be notified of a breach.** You have the right to be notified if a breach of your unsecured PHI occurs. We will notify you without unreasonable delay and in no case later than 60 days after we discover the breach.
- **Right to a paper copy of this Notice.** You can ask for a paper copy of this Notice at any time, even if you agreed to receive it electronically. You also have the right to a copy of any revised Notice.

To exercise any of these rights, contact our Privacy Officer using the contact information in Section 9.

9. Complaints

If you believe your privacy rights have been violated, or if you have questions or concerns about how we handle your protected health information, please contact our designated Privacy Officer / Practice Manager:

Archangel Michael Health, PA

Attn: Privacy Officer / Practice Manager

Phone: 352-441-9110 (request to speak with the manager or privacy officer)

Email: manager@archangelmichaelhealth.com

You may also file a complaint directly with the Office for Civil Rights (OCR) at the U.S. Department of Health & Human Services. **We will not retaliate against you in any way for filing a complaint.**

Online Complaint Portal: <https://ocrportal.hhs.gov/ocr/portal/lobby.jsf>

Mail: U.S. Department of Health & Human Services

200 Independence Avenue, S.W.

Room 509F, HHH Building

Washington, D.C. 20201

10. Changes to This Notice

Archangel Michael Health, PA reserves the right to change the terms of this Notice and to make the new provisions effective for all protected health information we maintain. If we make material changes, we will post the revised Notice on our website and provide a copy upon request. Acknowledgment of receipt of this Notice is collected as part of the new-patient intake form.

Questions & Contact

Archangel Michael Health, PA — Attn: Privacy Officer / Practice Manager

Phone: 352-441-9110 · Fax: 352-441-9114

Email: manager@archangelmichaelhealth.com

Website: <https://archangelmichaelhealth.com>

© 2026 Archangel Michael Health, PA · v2026.07.02