VERIMED HEALTH GROUP | PRIVACY

FINAL REVIEW DRAFT - PRIVACY / LEGAL / WEB

veriMED Health Group Website Privacy Policy

veriMED IPA, LLC d/b/a veriMED Health Group

Effective date: October 15, 2026

THIS POLICY DESCRIBES HOW VERIMED COLLECTS, USES, DISCLOSES, AND PROTECTS PERSONAL INFORMATION WHEN YOU USE OUR WEBSITES, APPLICATIONS, AND RELATED SERVICES. PLEASE REVIEW IT CAREFULLY.

Contents

1. Who veriMED is and when this policy applies
2. Information we collect
3. Website functions and third-party services
4. Cookies, analytics, advertising, and campaign measurement
5. How we use information
6. How we disclose information
7. Communications and consent
8. Your choices and privacy requests
9. Retention
10. Children's privacy
11. Data security
12. Changes to this policy
13. Contact us

1. Who veriMED is and When This Policy Applies

veriMED IPA, LLC d/b/a veriMED Health Group ("veriMED," "we," "us," or "our") is a health care provider organization within the Millennium Physician Group family of health care organizations. veriMED provides primary care information, clinic and provider resources, and patient-facing information through its public Website and related online experiences.

This Website Privacy Policy governs your access to and use of the veriMED Website.

For purposes of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the applicable veriMED covered entity participates in the affiliated covered entity described in the Millennium Healthcare Notice of Privacy Practices (the "NPP"). The NPP explains how participating health care entities may use and disclose

protected health information ("PHI") and describes patient rights. When information collected through the Website becomes PHI maintained by veriMED or another participating covered entity, the NPP and applicable health privacy laws govern that information.

Scope of this Website Privacy Policy

This Website Privacy Policy applies to verimedhealthgroup.com, clinic and location pages or subdomains operated for veriMED, and veriMED-branded landing pages, microsites, and campaign pages that link to this policy (collectively, the "Website"). It applies when you browse the Website, review provider or clinic information, interact with Website features, submit a Contact, Become a Patient, Annual Enrollment Period ("AEP"), clinic, or other public form, or communicate with veriMED in response to a Website request.

The Website is intended for general information and public-facing requests. It is not an emergency or clinical communication channel. Call 911 for an emergency. Current patients should contact their clinic or use an approved patient channel for medical questions, appointments, prescriptions, test results, or detailed clinical information.

What this policy does not cover

This policy does not govern information collected directly through a password-protected patient portal, medical record system, telehealth platform, or other secure health care environment. Such information may be PHI and is governed by the NPP and applicable law.

The Website may link to services operated by third parties, including mapping and directions services, social media platforms (e.g., Facebook/Meta), Medicare or health-plan resources, patient services, and other external resources. When you leave the Website or submit information directly to a third party, that service may have its own privacy policy and terms. A third party may also process information on veriMED's behalf under contractual, privacy, security, and HIPAA requirements, as applicable. Please note: **Social media platforms and external links do not act as HIPAA Business Associates on our behalf.**

2. Information We Collect

We collect information directly from you, automatically through the Website, and from approved affiliates or service providers when relevant to your request, a campaign, security, or another permitted business purpose. Depending on the context, information submitted to a health care provider may become PHI when it is maintained by veriMED in connection with health care.

Category	Examples
Identifiers and contact information	Name, e-mail address, telephone number, mailing address, and age or date-of-birth information when a form specifically requests it.
Prospective-patient and routing information	ZIP code, county, preferred clinic or provider, caregiver status, Medicare eligibility or enrollment-related responses when requested, insurance or service-area information, referral source, campaign source, and contact preferences.

Category	Examples
Inquiry and communication content	Messages, attachments, feedback, survey responses, and other information you choose to provide. General public forms are solely intended for general prospective-patient inquiries, scheduling requests, or contact preferences, not detailed clinical information.,
Internet and device activity	IP address, browser and device type, operating system, language, pages viewed, search activity, referral URL, campaign parameters, interactions with Website content, and form-submit or conversion events.
Approximate location and device context	Approximate location derived from IP address or device settings, local time, time zone, and similar technical context.
Consent and preference records	The notice or consent language displayed, its version or date, the source page or campaign, the time of submission, and the choices you make.
Service and referral information	Limited appointment-request, clinic, provider, insurance, referral, or service information received through a Website feature or supported service. Payment or medical-record information, when available through an external service, may be collected directly by that provider rather than veriMED.

How we collect information

- Directly from you when you complete a Website form, request information, communicate with us, participate in a survey, or otherwise provide information.
- Automatically through server logs, cookies, tags, analytics tools, campaign parameters, and similar technologies when you browse or interact with the Website.
- Through Website features and approved service providers that support clinic and location information, mapping, social content, patient resources, campaign measurement, security, and other Website functions.
- From affiliates, referral sources, campaign partners, and other permitted sources when relevant to a request, campaign, security function, or business purpose.

How Website forms are routed

Depending on the form and workflow, a submission may be delivered to authorized veriMED or clinic personnel for review and routing or transferred through approved MPG-controlled infrastructure to an approved customer relationship management or lead-management system. veriMED AEP “Become a Patient” landing-page forms use the separate integration described in this policy. Lead-form information is kept separate from the data used for advertising and analytics measurement.

3. Website functions and third-party services

The Website uses internal and third-party services to provide public information and connect users to supported resources. The service provider and data flow may vary by feature.

Function	Service / Provider	Purpose
Provider, clinic, and location information	veriMED Website; clinic pages and subdomains; Google Maps or approved mapping services	Displays clinic locations, provider and service information, hours, contact information, and directions.
Contact and Become a Patient forms	veriMED Website and approved form services	Collects information a visitor intentionally submits so veriMED can respond, route the request, or support a prospective-patient inquiry.
AEP lead intake and routing	MPG-controlled infrastructure; Salesforce	Creates and routes a brand-specific prospective-patient lead for requested follow-up by authorized internal teams.
Insurance and educational resources	veriMED Website and approved external links	Provides general provider, Medicare/AEP, accepted-plan, and health education information; external sites apply their own policies.
Social media content and links	Facebook / Meta and other approved social platforms	Displays or links to social content. Social platforms may receive technical and interaction information when their content is loaded or selected.
Analytics and campaign measurement	Google Analytics, Google Ads and Meta measurement tools, tag management, and MPG-controlled Google Cloud services	Measures Website use and approved campaign or conversion performance under the PHI-Free Tracking configuration described below.
Hosting, security, and Website operations	Approved hosting, cloud, content-management, and security providers	Supports Website delivery, availability, security, logging, troubleshooting, and maintenance.

4. Cookies, analytics, advertising, and campaign measurement

Cookies and similar technologies

We and our service providers may use session and persistent cookies, web beacons, tags, server logs, or similar technologies for Website operation, security, preferences, analytics, and approved campaign measurement. You can restrict or delete cookies through your browser and through a Website preference tool where one is provided. Some Website functions may not work as intended if cookies are disabled.

Approved measurement tools

Depending on the page and approved configuration, veriMED uses or may use Google Analytics, Google Ads conversion measurement, Meta measurement tools, tag management, conversion events, server logs, and similar technologies to understand Website use, attribute campaign sources, and measure whether a campaign led to a completed form or other approved action.

PHI-Free Tracking and sensitive-data protections

For the current veriMED Website, Website activity used for advertising or analytics measurement is routed first through MPG-controlled Google Cloud Platform services and related internal infrastructure. MPG controls what

data is permitted to be forwarded to downstream measurement providers. Advertising platforms do not directly collect the user-entered Website-form information addressed by this architecture.

The PHI-Free Tracking controls filter or block PHI, direct identifiers, user-entered form values, health-related information, and IP addresses before limited technical, event, and campaign-measurement data is forwarded to Google Analytics, Google Ads, Meta, or another approved provider. Approved browser-side tracking is configured so it does not read form fields or defeat the server-side filtering model.

Information intentionally submitted through an AEP lead form follows a separate approved path to Salesforce for lead creation, routing, and requested follow-up. That lead-data path is separate from advertising and analytics measurement.

Under the configuration, names, e-mail addresses, telephone numbers, free-text messages, Medicare or caregiver responses, consent records, and other Website-form values are not transmitted to advertising or analytics platforms. Tracking is used for internal campaign and conversion measurement only. Retargeting and remarketing, custom or lookalike audiences, uploaded patient or lead lists, and PHI-derived audience targeting are not enabled.

5. How we use information

- Operate, maintain, secure, troubleshoot, and improve the Website and its functions.
- Respond to inquiries and provide information, services, or resources you request.
- Create, route, and manage prospective-patient, AEP, or campaign leads and coordinate follow-up by authorized internal teams.
- Support provider, clinic, and location information, patient resources, contact pathways, insurance information, and other Website functions.
- Attribute campaign sources, measure conversions, evaluate Website content, and analyze aggregate Website use.
- Communicate with you through channels you request or authorize, subject to consent, preference, and suppression requirements.
- Provide newsletters, promotions, or marketing communications only where permitted and supported by any consent or authorization that may be required.
- Authenticate use, detect fraud or abuse, protect systems and users, investigate incidents, and enforce applicable terms.
- De-identify or aggregate information for analytics, reporting, planning, quality improvement, and other lawful purposes.
- Comply with law, legal process, regulatory obligations, contracts, audits, recordkeeping requirements, and other purposes disclosed when information is collected or with your consent.

6. How we disclose information

- **Affiliates and related health care organizations.** We may share information with Millennium Physician Group and other affiliated entities for legitimate business, administrative, operational, or health care purposes, subject to applicable law and the NPP when PHI is involved.

- **Vendors and service providers.** We may share information with providers that support hosting, cloud infrastructure, CRM and lead management, communications, analytics, advertising measurement, security, mapping, social integrations, customer support, Website operations, and other operational functions.
- **Authorized internal teams.** We may make information available to Community Partnership, Patient Engagement, clinic, outreach, grievance, or other authorized teams when needed to respond to or route a request.
- At your request or direction. We may share information with a health care provider, family member, caregiver, or other person you designate, or with a service you choose to use.
- **Analytics and advertising measurement providers.** We may disclose limited Website-event information under the PHI-Free Tracking configuration described in Section 4. We do not authorize disclosure of PHI or Website-form values to these providers for their own targeted advertising.
- Legal, compliance, safety, and business transactions. We may disclose information when required or permitted by law, to protect rights or safety, to respond to legal or regulatory process, or in connection with a merger, acquisition, restructuring, financing, or similar transaction subject to applicable obligations.
- De-identified or aggregated information. We may disclose information that has been processed so that it cannot reasonably be used to identify an individual, as permitted by applicable law.

Mobile and messaging information

veriMED does not sell mobile telephone numbers, text-message opt-in data, or communication-consent records, and does not disclose them to third parties for the third parties' own marketing or promotional purposes. Service providers may process such information only to support veriMED communications or another permitted service.

7. Communications and consent

The disclosure and choices displayed on a specific form control the communication you are requesting. Submitting a Become a Patient or AEP form may authorize veriMED to respond by manual telephone call or e-mail when the form says so. It does not, by itself, authorize unrelated future promotional messages, recurring marketing texts, or automated or prerecorded telemarketing calls.

- Requested follow-up. We may contact you by the channels described at the point of collection to respond to your request and discuss becoming a patient.
- Promotional e-mail. Where offered, a future promotional e-mail subscription is separate and optional. You may unsubscribe using the link in the message.
- **Text messages and automated calls.** veriMED will present separate channel-specific language and obtain any legally required consent before using recurring marketing texts or automated or prerecorded telemarketing calls.
- Text messaging Consent and Opt-Out. If you consent to receive text messages from veriMED (such as appointment reminders, prospective-patient outreach, or service updates), message and data rates may apply. You can opt out of receiving text messages at any time by replying STOP to any message you receive from us. For help, reply HELP or contact us using the details below. Opting out of marketing or informational texts will not prevent critical care-related notifications sent through approved patient communications channels.
- Preferences and suppression. You may ask veriMED to update communication preferences. We may retain limited suppression information needed to honor an opt-out or do-not-contact request.

8. Your choices and privacy requests

- Cookies and browser controls. Most browsers let you restrict or delete cookies. Where veriMED provides a Website preference tool, you may also use that tool.
- **Advertising choices.** The approved veriMED tracking configuration does not use retargeting or remarketing. Where other approved advertising technologies or Website preference controls provide choices, you may use those controls and applicable industry opt-out tools.
- E-mail. You may opt out of promotional e-mail using the unsubscribe mechanism in the message. This does not prevent service, transactional, legal, or care-related communications that are otherwise permitted.
- Telephone and other preferences. Contact veriMED or the Privacy Office to request an update to communication preferences or to ask that promotional contact stop.
- Access, correction, or deletion. You may request access to, correction of, or deletion of Personal Information collected through the public Website, subject to applicable law, verification, security, and recordkeeping obligations. Some information may not be eligible for deletion.
- **Medical records and HIPAA rights.** Requests concerning medical records, PHI, or HIPAA rights must be handled under the NPP and veriMED's patient-rights processes.

State privacy rights and browser signals

Depending on where you live, applicable law may provide additional rights regarding Personal Information. Some privacy laws exempt PHI, health care information, or entities regulated by HIPAA. We will evaluate a verified request and respond as required by applicable law. Some browsers transmit Do Not Track or opt-out preference signals. Because standards are not uniform, the Website may not respond to every signal, but veriMED will honor legally required signals where applicable and technically supported.

To the extent veriMED collects Personal Information through the public Website that is subject to applicable state privacy legislation, eligible residents may have the following rights:

- **Right to Access / Know:** Request confirmation of whether we process your Personal Information and request access to or a copy of the specific pieces of Personal Information we have collected about you in a portable, readily usable format.
- **Right to Correction:** Request that we correct inaccuracies in your Personal Information, taking into account its nature and the purpose of processing.
- **Right to Deletion:** Request the deletion of Personal Information provided by or collected about you, subject to statutory retention, legal, and operational exceptions.
- **Right to Opt-Out of Sale, Sharing, or Targeted Advertising:** Request to opt out of the "sale" of your Personal Information, sharing for cross-context behavioral advertising, or targeted advertising. *Note: veriMED does not sell Personal Information or share website activity with third parties for cross-context targeted advertising under our PHI-Free Tracking configuration.*
- **Right to Non-Discrimination:** Exercise any of your privacy rights without receiving discriminatory treatment or a denial of Website services.

Submitting a Request or Appeal. To exercise any applicable state privacy right, please submit a request to the Privacy Office using the contact details in Section 13. We will verify your identity before processing your request using standard security procedures. Authorized agents submitting requests on behalf of an eligible consumer must provide written proof of authorization. If we decline to take action regarding your request, we will inform you of our decision and the legal reason for it. If your state provides a right to appeal, you may appeal our decision within 30 days by writing to our Privacy Office with the subject line

"Privacy Request Appeal". If your appeal is denied, you may have the right to contact your state Attorney General.

9. Retention

We retain Personal Information for as long as reasonably necessary for the purposes described in this policy, including to respond to requests, manage leads and communications, honor preferences, maintain security and audit records, comply with legal and contractual obligations, resolve disputes, and enforce agreements. Retention periods may vary by information type, system, and business purpose. If information becomes part of a patient record or another regulated record, the applicable legal, clinical, records-management, and NPP requirements govern retention and disposition.

10. Children's privacy

The public Website is intended primarily for adults, patients, prospective patients, family members, caregivers, insurance partners, and other users seeking veriMED information and services. We do not knowingly collect Personal Information directly from children under 13 through general public Website forms without appropriate involvement of a parent or legal guardian, except where collection is otherwise permitted by law. A parent or legal guardian may use the Website on behalf of a minor. PHI involving a minor is governed by the NPP and applicable federal and state law.

11. Data security

veriMED uses administrative, technical, and physical safeguards designed to reduce the risk of accidental, unauthorized, unlawful, or improper access, alteration, disclosure, destruction, or use of information. Safeguards may include access restrictions, secure transmission, encryption, logging, monitoring, vendor controls, and other measures appropriate to the information and system involved.

No Internet transmission or electronic storage method is completely secure, and we cannot guarantee absolute security. Do not use a general public Website form to send emergency information, detailed clinical information, account credentials, or other information that the form does not request. If you believe information submitted through the Website may have been compromised, contact the Privacy Office using the information below.

12. Changes to this policy

We may update this policy to reflect changes in the Website, data practices, technologies, vendors, legal requirements, or organizational structure. We will post the updated policy on the Website and update the effective or revision date. If a change materially affects how we use Personal Information, we may provide additional notice where appropriate or required by law.

13. Contact us

Questions, concerns, complaints, or requests about this policy or veriMED's public Website privacy practices may be directed to:

Privacy Office	Mosaic Health / MPG / veriMED Health Group Privacy Office

Telephone	(855) 517-8676
E-mail	Privacy@mosaichealth.com
Website	verimedhealthgroup.com