Customer-Facing

Privacy Policy

How we collect, use, disclose, and protect information

VERSION	EFFECTIVE	OWNER
1.4	July 22, 2026	Ben Ehrlich, Security Officer

Contents

This Privacy Policy describes how Merza Medical, LLC ("Merza Medical," "we," "us," or "our") collects, uses, discloses, and protects information in connection with our ambient medical scribe application, Alfred, and related services (collectively, the "Services"). It applies to healthcare providers ("Providers") who use Alfred and to visitors to our website at merzamedical.com.

Merza Medical operates as a **Business Associate** under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"). We process Protected Health Information ("PHI") only on behalf of healthcare providers (Covered Entities) pursuant to Business Associate Agreements ("BAAs").

This Privacy Policy is NOT a Notice of Privacy Practices. It does not describe the privacy practices of any Covered Entity, and it does not govern our handling of PHI. **Our use and disclosure of PHI is governed solely by the applicable BAA between Merza Medical and the Provider, which controls in the event of any conflict with this Privacy Policy.** The sections below that describe PHI processing are provided for transparency only; they do not create rights or obligations beyond the BAA.

If you are a patient, your healthcare provider (the doctor or clinic using Alfred) is the Covered Entity responsible for providing you with a Notice of Privacy Practices and for responding to requests about your health information. Please contact your healthcare provider directly. You may also reach us at admin@merzamedical.com, and we will coordinate with your provider.

1 Information We Collect

1.1 PROTECTED HEALTH INFORMATION (PHI)

When a Provider uses Alfred to document a clinical encounter, we process the following categories of PHI on that Provider's behalf, under the BAA:

- **Audio recordings** of clinician-patient encounters
- **Transcripts** generated from those recordings
- **Clinical notes** generated from transcripts, including draft diagnostic (ICD-10) and observation (LOINC) codes
- **Patient demographic information** entered by the Provider (e.g., patient name, date of birth, medical record number)

- **Metadata** associated with the above, such as encounter date and recording duration

Our handling of this PHI is governed by the BAA, not this Privacy Policy.

1.2 PROVIDER ACCOUNT INFORMATION

When a Provider registers for Alfred, we collect:

- **Identity data:** Full name, professional title, medical license information
- **Contact data:** Email address, phone number
- **Authentication data:** Login credentials (passwords are never stored in plaintext)
- **Practice data:** Clinic or practice name, specialty, NPI number (if provided)
- **Billing and subscription data:** Subscription plan, price, quantity or seat count, billing contact, subscription and transaction status, limited masked payment-method details (such as card brand and last four digits), and references assigned by our payment processor. Payment credentials are submitted directly to our payment processor; our Services are not designed to receive or store full card or bank-account numbers.
- **Subscription-consent records:** The version and content of the offer and terms presented, the action taken to accept them, date and time, account and organization identifiers, technical evidence such as IP address and user agent, checkout and subscription references, and delivery of the subscription acknowledgment. We use this information to document the subscription agreement, process cancellation requests, resolve disputes, and comply with law.

1.3 TECHNICAL AND USAGE DATA

We automatically collect limited technical data necessary to operate and secure the Services:

- **Device information:** Device type, operating system version, app version
- **Log data:** Access logs, error logs (sanitized to exclude PHI), authentication events
- **Usage data:** Feature usage patterns, session duration, number of encounters processed (aggregated, not tied to individual patients)

What we do NOT collect: We do not use analytics SDKs, crash-reporting tools, advertising trackers, or any third-party tools that could capture PHI. We do not collect data from patients directly — all PHI flows through the Provider's use of Alfred.

2 How We Use Information

2.1 PHI — PERMITTED USES

We use PHI solely as authorized by the applicable BAA and as permitted by HIPAA — to transcribe encounter audio, generate clinical notes with draft diagnostic and observation codes, display notes for the Provider's review and export, support patient data access/amendment/deletion requests as directed by the Provider, and maintain audit logs. **The BAA governs; this section is descriptive only.**

We do NOT use PHI for marketing or advertising; training or improving any machine-learning or artificial-intelligence model; sale to any third party; or any purpose not authorized by the applicable BAA and HIPAA.

2.2 PROVIDER ACCOUNT INFORMATION

We use provider account information to create and manage accounts, authenticate providers and enforce access controls, communicate about the account and service/security updates, process payments and manage subscriptions, and comply with legal obligations.

2.3 TECHNICAL AND USAGE DATA

We use technical and usage data to operate, maintain, and improve the Services; monitor performance and security; detect and prevent fraud, unauthorized access, and security incidents; and generate aggregated, de-identified analytics (which do not constitute PHI or personal data).

3 How We Process PHI

When a Provider records a clinical encounter, Alfred processes the encounter audio to produce a transcript and a structured clinical note — including draft diagnostic and observation codes — which the Provider reviews and exports to their record system. This processing is performed with the assistance of the subprocessors identified in

Section 4, each bound by a BAA and operating within the United States, and is protected by the safeguards described in Section 6. This overview is descriptive only; our handling of PHI is governed by the applicable BAA.

AI-generated content and clinician review. Clinical notes produced by Alfred are generated with the assistance of artificial intelligence. **AI-generated clinical notes are drafts that require clinician review and verification before they may be used in patient care or incorporated into the medical record.** Merza Medical does not represent that AI-generated content is a substitute for clinical judgment; the Provider bears sole responsibility for the accuracy and completeness of any note they adopt. See the AI Disclaimer in our Terms of Service.

4 Subprocessors and Third-Party Services

We use a small number of subprocessors to deliver the Services. Each subprocessor that handles PHI is bound by an executed BAA and processes data within the United States:

Subprocessor	Role
Amazon Web Services	Cloud infrastructure
AssemblyAI, Inc.	Medical transcription
Anthropic, PBC	AI note generation

A current list of subprocessors is available on request. We do **not** use customer data — audio, transcripts, or notes — to train artificial-intelligence models, and no subprocessor uses it to train or improve its models.

We do not share PHI with any subprocessor not listed above. If we engage an additional subprocessor that will handle PHI, we will update this Privacy Policy and provide advance notice as required by our BAAs — including any right to object — before that subprocessor begins processing PHI.

Where a Provider connects an optional integration, it operates only at the Provider's direction and under the same safeguards.

Payment processing. We use Stripe, Inc. as our third-party payment processor to bill subscription Fees and manage subscriptions. Stripe receives Provider account, billing, transaction, and payment-method information and processes it under our agreement with Stripe and the Stripe Privacy Policy, including for the purposes described there. We receive subscription and transaction identifiers and status, plus limited masked payment-method information needed to administer the subscription; our Services are not designed to receive full card or bank-account numbers.

Our billing workflow is intentionally separated from patient encounters: **Stripe is not used as a HIPAA subprocessor, and we configure the workflow so that patient encounter data and PHI are not sent to Stripe.** Providers must not enter patient information or PHI in billing names, descriptions, invoice notes, metadata, support requests, or other payment fields. If we materially change the workflow so Stripe would handle PHI on our behalf, we will first reassess the arrangement under HIPAA and update the applicable agreements and disclosures.

5 Data Retention and Deletion

5.1 RETENTION PERIODS

- **Audio recordings:** Retained under a 7-year lifecycle, consistent with medical-record retention requirements in most U.S. states.
- **Transcripts and clinical notes:** Retained for the duration of the Provider's account, plus the applicable retention period.
- **Provider account data:** Retained for the duration of the active account, plus a 30-day grace period after deletion is initiated.
- **Billing, transaction, and subscription-consent records:** Retained while the subscription or related payment remains active and afterward for the period reasonably necessary for accounting, tax, fraud prevention, dispute resolution, contract enforcement, and proof of consent, including any longer minimum period required by applicable law. These records do not include full payment credentials.
- **Audit logs:** Retained for compliance purposes (metadata only; no PHI content).
- **Technical logs:** Retained up to 90 days for operational and security purposes.

5.2 ACCOUNT DELETION

Providers may delete their account at any time:

- **Self-service:** Settings > Delete Account in the Alfred iOS app, which immediately disables the account and starts a 30-day grace period.
- **Email request:** Contact admin@merzamedical.com.

During the grace period the account is disabled and its data retained but inaccessible; the Provider may contact us to reverse the deletion. After 30 days, patient records and clinical notes, audio recordings, and the active account profile are permanently deleted, subject to the BAA and applicable legal retention obligations. Audit-log entries (no PHI content) are retained for compliance, and the limited billing, transaction, and subscription-consent records described in Section 5.1 may be retained after account deletion for the stated purposes. Those retained records cannot be used to access the deleted account.

5.3 DATA MINIMIZATION

We collect and retain only the data necessary to provide the Services, and no longer than required by our contractual obligations and applicable law.

6 Data Security

We implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and other data, consistent with the HIPAA Security Rule (45 CFR Part 164, Subpart C, as amended from time to time). We maintain a written HIPAA security program and host the Services on a HIPAA-eligible cloud provider whose infrastructure is independently audited under recognized security standards. (Merza Medical does not itself hold a SOC 2, ISO 27001, or HITRUST certification; its cloud provider does, and Merza operates a written HIPAA program with SOC 2-aligned controls.)

6.1 TECHNICAL SAFEGUARDS

- **Encryption:** Data is encrypted in transit and at rest.

- **Authentication:** Authenticated access with session controls and multi-factor authentication.
- **Access control:** Each Provider can access only their own patients' data.
- **Audit logging:** System and application activity is logged for audit and monitoring.
- **Threat detection:** Continuous monitoring and security alerting.
- **Error handling:** Error logging is sanitized to keep PHI out of log output.

6.2 ADMINISTRATIVE SAFEGUARDS

- HIPAA Security Risk Analysis conducted and documented
- Written HIPAA policies and procedures
- Workforce HIPAA training with documented acknowledgment
- Incident Response Plan and Breach Notification Plan
- Sanction policy for policy violations
- Change-management procedures for system updates

6.3 PHYSICAL SAFEGUARDS

All data is stored with a HIPAA-eligible cloud provider whose data centers maintain independent security attestations, physical access controls, 24/7 security, and environmental protections. No PHI is stored on Merza Medical's own premises or servers.

7 PHI Rights and Provider Rights

7.1 PATIENT RIGHTS UNDER HIPAA

Patients whose encounters are processed through Alfred retain all rights guaranteed by the HIPAA Privacy Rule, including Access (45 CFR §164.524), Amendment (§164.526), Accounting of Disclosures (§164.528), and Restrictions (§164.522). **These rights are administered by the patient's healthcare provider (the Covered Entity), not by Merza Medical, and are governed by the BAA — not by this Privacy Policy or by state consumer-privacy law.** If a patient contacts us directly, we will coordinate with

the applicable Provider. Our Patient Data Request Procedures document details the process.

7.2 PROVIDER RIGHTS

As a Provider using Alfred, you may access the account data and PHI processed on your behalf, correct inaccurate account information, delete your account and associated data (subject to applicable retention requirements), export your data in a portable format, and withdraw from the Services by terminating your account.

8 State Privacy Rights (Non-PHI Personal Data Only)

PHI that Merza Medical processes under HIPAA is **exempt** from U.S. state consumer-privacy laws — including the California Consumer Privacy Act/California Privacy Rights Act (Cal. Civ. Code §1798.145(c)(1)(A)), the Oregon Consumer Privacy Act (ORS 646A.570 et seq.), and comparable laws — because it is processed by a Business Associate governed by HIPAA. This exemption covers all patient encounter data (audio, transcripts, notes, and associated metadata).

The rights below therefore apply **only to non-PHI personal data** we control — such as Provider account information and website/usage data. Residents of states with a **data-level** HIPAA exemption (currently including California, Colorado, Oregon, Minnesota, New Jersey, and Delaware) may exercise these rights as to that residual data:

- **Know / Access** — what personal data we collect, how it is used, and a copy of it
- **Correct** — inaccuracies in your personal data
- **Delete** — your personal data
- **Opt out of the sale or sharing of personal data, and of targeted advertising and profiling** — note that **we do not sell or share personal data, do not deliver targeted advertising, and do not engage in profiling that produces legal or similarly significant effects**

Do Not Sell or Share My Personal Information / Global Privacy Control. We do not sell or share personal data, so no opt-out is necessary; nonetheless, we honor opt-out preference signals, including the **Global Privacy Control (GPC)**, where legally required.

Authorized agents. You may use an authorized agent to submit a request on your behalf; we may require the agent to demonstrate authority and may verify your identity directly.

Appeals. If we deny a rights request, you may appeal by replying to our decision or contacting privacy@merzamedical.com; we will respond within the time required by applicable law. If your appeal is denied, you may contact your state Attorney General.

Some states (including Virginia, Texas, Utah, Connecticut, and Florida) exempt HIPAA-regulated entities and/or business associates at the **entity level**; where such an exemption applies, Merza Medical is exempt from that state's consumer-privacy law in full, and this Section 8 does not create additional rights.

To exercise any right, contact privacy@merzamedical.com. We will respond to verified requests within the period required by applicable law (generally 45 days).

9 Disclosures of Information

We may disclose information only in these limited circumstances:

- **To the Provider** who created it.
- **To PHI subprocessors** (Section 4), solely to provide the Services and subject to BAAs.
- **To payment and billing providers** (Section 4), to process payments and administer subscriptions using Provider account and billing data, not PHI.
- **As required by law** — to comply with applicable laws, legal process, or enforceable governmental requests, including HIPAA-required disclosures to the U.S. Department of Health and Human Services (HHS).
- **To protect rights and safety** — where necessary to protect our rights, your safety, or the safety of others, or to investigate fraud.
- **Business transfers** — in connection with a merger, acquisition, or sale of assets, provided the successor is bound by this Privacy Policy and the applicable BAAs.

We do NOT sell, rent, or trade PHI or personal data to any third party for any purpose.

10 Breach Notification

In the event of a breach of unsecured PHI, Merza Medical will comply with the HIPAA Breach Notification Rule (45 CFR §§164.400–414) and its BAA obligations. As a Business Associate, we notify the affected Provider (Covered Entity) **without unreasonable delay and no later than 60 calendar days after discovery** (45 CFR §164.410); the applicable BAA may specify a shorter notification period, which controls. We cooperate with the Provider's patient notifications and assist with any required reporting to HHS or media. The Provider, as Covered Entity, is responsible for notifying affected individuals. Our Incident Response Plan and Breach Notification Plan are available to Providers upon request.

11 Cookies and Tracking Technologies

The Alfred web dashboard uses only essential cookies and session storage required for authentication and security. We do **not** use advertising or marketing cookies, third-party analytics tools, cross-site tracking pixels or beacons, or social-media tracking integrations. Our content delivery network may set functional cookies for performance and security; these contain no PHI and are not used for tracking or profiling.

12 Children's Privacy

The Services are for licensed healthcare providers and are not directed at individuals under 18. We do not knowingly collect personal data from children. Any PHI that incidentally concerns a minor patient is handled under HIPAA and the applicable Provider's obligations, not under COPPA, because the Provider — not the minor — is our user.

13 Data Location and International Transfers

PHI processed through Alfred is stored and processed within the **United States**, and our PHI subprocessors process it within the United States. Non-PHI Provider account and billing data may be processed by Stripe or another non-PHI service provider in the countries where that provider operates, subject to its contractual and legal safeguards. If you access the Services from outside the United States, you understand that your information will be transferred to and processed in the United States and, for non-PHI account or billing services, potentially in other countries disclosed by the applicable provider.

14 Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices, technology, or legal requirements. When we make material changes, we will update the "Last Updated" date, notify active Providers by email or in-app notice, and, where changes materially affect PHI handling, provide advance notice as required by our BAAs. Continued use of the Services after the effective date constitutes acceptance of the changes. No change to this Privacy Policy modifies the applicable BAA, which can be amended only by written agreement of the parties.

15 Contact Information

Role	Contact	Details
Privacy Officer / General Inquiries	Merza Medical, LLC	admin@merzamedical.com
Privacy Rights (CCPA/OCPA and other state laws)	Merza Medical, LLC	privacy@merzamedical.com

Role	Contact	Details
Phone	Merza Medical, LLC	971-712-4907

If you believe your privacy rights have been violated, you may file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, at https://www.hhs.gov/ocr/complaints/.

16 Governing Law

This Privacy Policy is governed by the laws of the State of Oregon and applicable federal law, including HIPAA. Any disputes arising from this Privacy Policy are subject to the exclusive jurisdiction of the state and federal courts located in Oregon. Where this Privacy Policy conflicts with a signed Business Associate Agreement or master services agreement, that agreement controls.

This document is a template provided for informational purposes and does not constitute legal advice. Consult qualified counsel regarding your specific obligations.

Merza Medical, LLC | Portland, Oregon, USA | admin@merzamedical.com | 971-712-4907

Change Log

Date	Change
2026-03-31	Initial publication
2026-04-04	Minor language updates
2026-05-25	Subprocessor and U.S. data-residency clarifications

Date	Change
2026-06-05	Subprocessor compliance-status update
2026-07-09	Compliance, state-privacy-rights, and editorial updates
2026-07-20	Added a billing-data category and a payment-processor (Stripe) disclosure for subscription billing and documented the intended separation between payment processing and PHI
2026-07-22	Added subscription-consent records, payment-provider privacy and international-processing disclosures, billing-record retention, and a requirement to keep PHI out of all billing fields