

REFERFLOW PRIVACY POLICY (PILOT PHASE)

Last Updated: December 6, 2025

ReferFlow, Inc. (“ReferFlow,” “we,” “us,” or “our”) provides a secure, cloud-based communication and referral workflow platform designed for image-based medical specialties. This Privacy Policy describes how ReferFlow collects, uses, discloses, and safeguards information during the Pilot Phase of the ReferFlow platform (the “Services”).

This Privacy Policy applies only to the Pilot Phase and only to users located in the United States. The Pilot is limited to healthcare organizations and licensed medical professionals in Illinois.

By accessing or using the Services, Customer and its Authorized Users acknowledge that they have read and understood this Privacy Policy.

1. Relationship to HIPAA and the Business Associate Agreement (BAA)

ReferFlow acts as a Business Associate to covered entities and their workforce members. When Customer uploads, transmits, or stores protected health information (“PHI”) within the Services, the handling of that PHI is governed by the HIPAA Privacy, Security, and Breach Notification Rules and the Business Associate Agreement (“BAA”) executed between ReferFlow and Customer.

If this Privacy Policy conflicts with the BAA regarding PHI, the BAA controls. This Privacy Policy does not replace the BAA.

2. Information We Collect

2.1 Information Provided by Customer or Authorized Users

ReferFlow collects information that Customer or its Authorized Users choose to upload, submit, or transmit through the Services, including names, email addresses, user credentials, diagnostic images, clinical notes, referral details, internal messages, and other information needed to use the Services.

2.2 Protected Health Information (PHI)

PHI may include medical images, clinical notes, referral details, and any patient identifiers contained in Customer’s content. ReferFlow processes PHI solely as permitted under HIPAA and the BAA and only to provide or support the Services.

2.3 Technical and Usage Information

ReferFlow automatically collects technical data such as device identifiers, browser type, IP address, authentication logs, timestamps, platform usage events, performance metrics, and security telemetry. This information helps maintain, secure, and improve the Services.

ReferFlow does not engage in behavioral advertising or cross-site tracking.

3. How We Use Information

ReferFlow uses information, including PHI, only for purposes permitted by Customer and applicable law. These purposes include providing the Services; facilitating referral workflows; securing the platform; monitoring performance; responding to technical issues; creating de-identified data for analytics or service improvement; complying with regulatory requirements; and communicating with Customer regarding the Pilot, including operational and administrative notices and limited non-PHI marketing emails.

ReferFlow does not use PHI for marketing.

4. How We Share Information

ReferFlow does not sell or rent Customer Data or PHI. ReferFlow shares information only as described below.

4.1 Customer-Directed Sharing

Information, including PHI, is shared only as instructed by Customer or its Authorized Users through the Services. This may include sharing with referral recipients, partner providers, or other authorized team members.

4.2 Subprocessors

ReferFlow uses subprocessors to host, support, and maintain the Services. Subprocessors receive only the minimum data necessary and are bound by contractual obligations to protect Customer Data and PHI.

4.3 Legal and Security Disclosures

ReferFlow may disclose information if required to comply with law, respond to law enforcement requests, comply with court orders or regulatory inquiries, enforce our agreements, protect the rights or safety of ReferFlow or others, or investigate fraud, abuse, or security threats. Any disclosure of PHI will comply with HIPAA and the BAA.

4.4 Corporate Transactions

If ReferFlow undergoes a merger, acquisition, financing, or sale of assets, Customer Data may be transferred to the acquiring or successor entity, subject to compliance with HIPAA and the BAA.

5. De-Identified and Aggregated Information

ReferFlow may create, use, and disclose de-identified data that meets HIPAA's de-identification standard. This data may be used for analytics, service improvement, operational insights, statistical reporting, and other lawful purposes. ReferFlow will not attempt to re-identify such data.

6. Data Retention and Deletion

ReferFlow retains Customer Content only as long as necessary to provide the Services, meet legal obligations, or fulfill the purposes described in this Privacy Policy.

At the end of the Pilot or upon termination, Customer may request an export of its data for a period of thirty (30) days. ReferFlow will delete Customer Content within sixty (60) days after the export period ends, except where retention is required by law or permitted for audit, backup, or security purposes. PHI will be handled in accordance with HIPAA and the BAA.

7. Security

ReferFlow maintains a comprehensive information security program designed to protect Customer Data and PHI. Security measures include encryption in transit and at rest, access controls, logging and monitoring, vulnerability management, and employee training. While ReferFlow uses reasonable safeguards, no system can guarantee absolute security.

8. Communications

ReferFlow may send transactional emails, administrative notices, and limited marketing communications during the Pilot. Marketing emails will not contain PHI and will include an opt-out mechanism. ReferFlow does not send SMS messages during the Pilot.

9. Children's Privacy

The Services are not intended for minors and may not be used by individuals under eighteen (18). ReferFlow does not knowingly collect personal information from children.

10. International Use

The Pilot is limited to users located in the United States. ReferFlow does not intentionally transfer Customer Data or PHI outside the United States during the Pilot. If international data

processing is implemented in the future, ReferFlow will provide appropriate notice and safeguards.

11. Your Privacy Rights

Because the Services are used solely by business entities and licensed professionals for professional purposes, and because ReferFlow acts as a Business Associate, consumer privacy rights laws such as the California Consumer Privacy Act (CCPA/CPRA) generally do not apply to Customer's use of the Services. Requests relating to PHI must be directed to the Covered Entity, not to ReferFlow.

12. Changes to This Privacy Policy; Contacts

ReferFlow may update this Privacy Policy to reflect changes in the Services, legal requirements, or operational practices. For material updates, ReferFlow will provide advance notice as required by law or agreement. Continued use of the Services after such updates take effect constitutes acceptance of the revised Privacy Policy.

If you have questions about this Privacy Policy or ReferFlow's data practices, please contact:

ReferFlow, Inc. – Privacy Office
919 N. Market Street, Suite 725. Wilmington, County of New Castle, Delaware 19801,
privacy@referflowapp.com

For HIPAA-related inquiries, please contact:

ReferFlow – HIPAA Compliance Officer: hipaa@referflowapp.com