Data Privacy & Data Management Policy

Effective: June 27, 2025 | Last Reviewed June 27, 2025

At Kermit PPI, safeguarding sensitive healthcare and operational data is a top priority. This comprehensive Data Privacy and Management Policy outlines how we collect, use, store, classify, protect, and retain information in alignment with applicable regulations such as HIPAA and organizational best practices. We are committed to maintaining transparency, confidentiality, integrity, and availability across all our data assets and supporting systems.

1. Scope

This policy applies to all data processed by Kermit PPI across our systems, including Snowflake, Kermit, SharePoint, Office 365, HubSpot, Confluence, Atlas, Jira, and Slack. It covers all categories of information from clients, vendors, and internal operations.

2. Data Privacy Policy (Collection, Storage, Archival & Purge)

Kermit PPI collects only the minimum necessary data to support our services and operations. All data is securely stored with access restrictions enforced by a role-based access control model. Our data governance framework—aligned with Snowflake's Enterprise Data Warehouse (EDW) capabilities—ensures traceable data lineage, documented access permissions, and the elimination of production data from test environments. Test datasets are anonymized to ensure compliance with privacy standards.

Archival and purge practices are governed by **KermIT Archive & Purge Policy KP-3**, applied across systems including Snowflake, Kermit, and SharePoint.

3. Information We Collect

- **Operational Data:** Case and billing data, implant product info, vendor invoice details, and procedure-level information.
- **User Data:** Names, email addresses, roles, and credentials of platform users.
- **System Data:** Logs, device types, access timestamps, and IP addresses.

We do **not** collect personal health information (PHI) unless explicitly authorized through a Business Associate Agreement (BAA).

4. Use of Information

Data collected is used to:

- Facilitate PPI case processing and vendor management
- Deliver platform functionality and client support
- Perform analytics and reporting
- Enhance system performance and security
- Fulfill legal and contractual obligations

We do not sell or disclose personal or proprietary data to third parties for marketing purposes.

5. Data Classification and Handling Policy

All data within Kermit systems is classified into one of three categories:

- **Public** – Non-sensitive data approved for public disclosure
- **Confidential** – Internal-use information with moderate sensitivity
- **Restricted** – Sensitive data requiring the highest level of protection

Restricted data is not shared externally without formal authorization. All employees undergo training to ensure proper handling based on classification. Systems in scope include Kermit, HubSpot, Confluence, Atlas, and Jira.

6. Data Backup and Retention Policy

We maintain daily backups of all critical data, with regular testing of restore processes performed quarterly. Backups are stored securely offsite with encryption. Retention policies follow HIPAA and HHS guidelines. Performance metrics such as backup success rates and recovery times are actively monitored.

Applicable systems: Kermit, Snowflake, Office 365, SharePoint.

7. Data Breach Policy

All data breach incidents are handled in accordance with Kermit's documented **Data Breach Procedures Plan**. This includes prompt detection, isolation, notification to affected parties, and remediation. Annual simulations are conducted to validate our incident response readiness.

Applicable systems: Kermit, Snowflake, Slack.

8. Data Governance Policy

Kermit maintains a formal **Data Governance Policy** to ensure:

- Clear ownership and stewardship of data assets
- Consistent metadata and lineage documentation
- Quality assurance and compliance with internal standards
- Enforcement of access control policies to maintain integrity and traceability

Snowflake and Kermit serve as the core platforms for governance oversight.

9. Security Practices

- Encrypted data in transit and at rest
- Multi-factor authentication (MFA)
- Granular role-based access control (RBAC)
- Regular third-party security reviews and vulnerability assessments
- HIPAA-compliant infrastructure and workflows

10. Your Rights and Requests

Clients and authorized users may request:

- Access to their data
- Corrections to inaccurate information
- Data deletion in accordance with contractual or legal guidelines

Contact: **privacy@kermitppi.com**

11. Policy Updates

This policy is reviewed and updated regularly to reflect legal changes, client requirements, and system enhancements. Clients will be notified of material changes in advance.

12. Contact Information

Kermit PPI – Privacy and Compliance Team
10807 Falls Rd.
PO Box 685
Brooklandville, MD 21022
Email: **privacy@kermitppi.com**
Phone: 888-568-4248