PURECHART

Data Retention and Disposal Policy

Company: Purechart AI LLC
Effective Date: March 2026
Policy Owner: Management / IT Administrator
Review Frequency: At least annually

---

1. Purpose

This Data Retention and Disposal Policy establishes guidelines for retaining, protecting, and securely disposing of company and customer information. The purpose is to retain information only for as long as necessary for legitimate business, legal, regulatory, and operational purposes.

2. Scope

This policy applies to company employees, contractors, systems, applications, databases, cloud services, and other storage locations that contain company, customer, patient, financial, or other confidential information.

3. Data Retention

The Company retains information only for the period necessary to fulfill the purpose for which it was collected or to satisfy applicable legal, regulatory, accounting, contractual, or business requirements.

Where applicable, retention periods may include:

- **Patient and healthcare records:** Retained in accordance with applicable healthcare and legal record-retention requirements.
- **Financial and transaction records:** Retained as required for accounting, tax, audit, and legal purposes.
- **Customer and application data:** Retained for as long as reasonably necessary to provide services, maintain the customer relationship, meet contractual obligations, or satisfy legal requirements.
- **Authentication and security logs:** Retained for a reasonable period necessary for security monitoring, troubleshooting, auditing, and investigation.
- **Temporary or unnecessary data:** Deleted or securely disposed of when it is no longer required.

Retention periods may vary depending on the type and sensitivity of the information.

4. Data Disposal

When information reaches the end of its required retention period, the Company will securely dispose of or delete the information in a manner appropriate to its sensitivity.

Electronic information may be securely deleted from systems and storage devices using appropriate deletion or sanitization procedures. Physical records containing confidential information will be securely destroyed, such as through shredding or an appropriate secure destruction service.

Where data is maintained by a third-party service provider, the Company will rely on the provider's documented data deletion and disposal procedures in accordance with applicable agreements and requirements.

5. Legal Holds

Information subject to a legal hold, investigation, audit, litigation, or other legal requirement will not be deleted or destroyed until the applicable hold or requirement has been released.

6. Responsibilities

Management and designated IT personnel are responsible for implementing and maintaining appropriate data-retention and disposal procedures. Employees and contractors must follow company requirements for handling, storing, and disposing of confidential information.

7. Review

This policy will be reviewed periodically and updated as necessary to reflect changes in the Company's systems, business operations, contractual obligations, and applicable legal or regulatory requirements.