Data Protection Policy & Audit Trail Documentation

PharmaSmart KE

This document outlines the data protection policies and audit trail capabilities of the PharmaSmart KE Pharmacy Management System.

1. Data Protection and Access Control

The system is designed with role-based access control (RBAC) to ensure data is only accessible to authorized personnel.

1.1. User Roles

Access is segregated into three distinct roles: Inventory, Sales, and Admin.

1.2. Authentication

Each user must select their role and enter an assigned password to log in to the system.

1.3. Password Management

The administrator has the ability to change user passwords, ensuring credential security.

2. Data Management and Retention

The system includes tools for the proper management, backup, and deletion of sensitive data.

2.1. Database Backup and Restore

The Admin role can perform database backups and restorations to prevent data loss and ensure business continuity.

2.2. Data Deletion

Administrators are authorized to clear old sales records from the system. A full factory reset option is also available to permanently erase all data.

2.3. Compliance and Retention

The system is designed to meet legal requirements for controlled substances. The DDA register feature generates records that must be stored securely by the pharmacy for a minimum of two years.

3. Sensitive Data Handling

The PharmaSmart KE system processes several categories of sensitive information, including:

- **Sales Data:** Records of each sale, including product, quantity, and price.
- **Controlled Substance Records (DDA):** A legally required register for controlled medicines that includes transaction date, medicine name, batch number, quantity sold, and dispenser information.
- **Patient Information:** The DDA register captures sensitive patient data, including the patient's name, prescriber, and prescription number.

4. Audit Trail and System Logging

To ensure accountability and traceability, the system maintains comprehensive logs of user activities.

4.1. Log Accessibility

The administrator has the exclusive ability to view and export system logs.

4.2. Logged Activities

While the specific log contents are not detailed, the system's functions imply that the audit trail captures critical actions such as:

- User logins and authentication events.
- Inventory modifications (additions, edits, deletions).
- Sales transaction entries.
- Generation of sales reports and DDA records.
- Administrative actions, including password changes, data clearing, backups, and factory resets.