LakePharma
The Biologics Company

LakePharma DPM System Overview and Security Whitepaper

(NR-6793)

April 2021

I. Introduction

LakePharma DPM (current version 5.81) is a data and process management system developed for LakePharma using RENKOM's RTS development platform. DPM is highly customizable by system administrators in LakePharma, and new functionalities are under continuous development by RENKOM.

II. Overview

The DPM system is LakePharma's unique cloud-based software platform that centralizes all of the company functions including ERP, CRM, LIMS and quality systems. The DPM acts as a centralized store of scientific data, company policies and financial information. The DPM's extensive permissions systems ensure that access is restricted for employees to what is relevant to them.

The DPM includes an easy-to-use client portal and LakePharma admins are able to extensively customize what level of information is released to clients.

The DPM is a unique software platform not only in the breadth of the activities and information consolidated in it, but also in the extensive audit trail that is a core feature of DPM and that is applicable to all parts of it. All user actions, not just those in specific modules, are securely recorded and timestamped, and searchable via the application frontend for users with the required permissions.

The DPM's extensive API allows integration with other software, and the integrated OAUTH server allows unified login and permissions across LakePharma properties.

The DPM is GMP ready: at least 15 DPM tables have been validated for use in GMP operations (21CFR11). Auditors have been consistently impressed by how the DPM enables staff to pull audit information quickly and easily.

III. Architecture and Design

- The LakePharma DPM is an entirely cloud-based web application hosted on Amazon Web Services (AWS). The application is developed primarily in Zend Framework with database storage in MySQL (AWS RDS Instances).

- As of DPM Version 5.71, The DPM's codebase has been segmented to improve security. System configuration code (RENKOM's RTS) is stored on a different server in a different AWS account that the system servers. All changes to system configuration must be done via API communication with the configuration server.

IV. Access Control

- The webserver is not exposed to the world and is only accessible via a bastion host on the same secure subnet. SSH access to the bastion host is restricted to IPs associated with the software development team.
- The MySQL database is not exposed to the world and can only be accessed by machines in the same secure subnet (IE the webserver).

V. Authentication

- Application users are required to have a password that includes both numbers and letters and is 8-23 characters long.
- Users are required to change their password at least once every year.
- Multi-Factor Authentication can be enabled for any user.
- Application administrators are required to have Multi-Factor Authentication enabled.
- Users are able to securely recover their username and password.

VI. Configuration Management

- System hardening has been performed on production systems
- There is a secure build process. Development is performed by an ISO 27001:2013 certified company. The development team utilizes website filtering and reviews user access rights and group policies regularly. Random audits of USB/storage devices are performed. Security Authentication Control has been implemented on JIRA and the private Github server, and activity logging and monitoring of Github and JIRA are carried out on a monthly basis.

VII. Cryptography

- All Database (MySQL) data is protected with encryption at rest.
- All application resources are encrypted through 256-bit TLS encryption.

VIII. Patch Management

- Patches are deployed via GIT and regression testing of all application functionality occurs after every patch.

IX. Proactive Monitoring

- DPM Contains an extensive audit trail detailing all created, edited and deleted information by all users including administrative actions.
- System logs are rotated nightly and stored on a Zabbix server for nightly review and analysis by the DPM development team. Email alerts are sent to the development team by the Zabbix server if any unusual activity is discovered.

- Application logs are rotated hourly and stored for seven days before deletion.
- Reviews of the audit, system and application logs are conducted quarterly in order to detect irregularities, including misuse of computing and application resources.
- SOPs for system administration are in place including an Intrusion Response Plan.
- The DPM application itself allows administrators to monitor application usage and set permissions levels within application. For example, the DPM allows administrators to:
    - Set up data-driven alerts and email notifications within the application.
    - Customize the application to require users to re-enter their password for sensitive/restricted table and record views, or to require a digital signature to confirm their identity when making edits to important record fields.
    - Program the application to restrict records and tables to specific individuals and groups, or with data-driven criteria-based permissions.

X. Backup and Resiliency

- The system database RDS instance is backed up nightly and these snapshots are retained within AWS for at least 30 days.
- The system server disk is backed up weekly and these backups are retained within AWS for at least 1 year.

CONTACT

Abby Kochavi

Senior Director, Operations

abby.kochavi@lakepharma.com