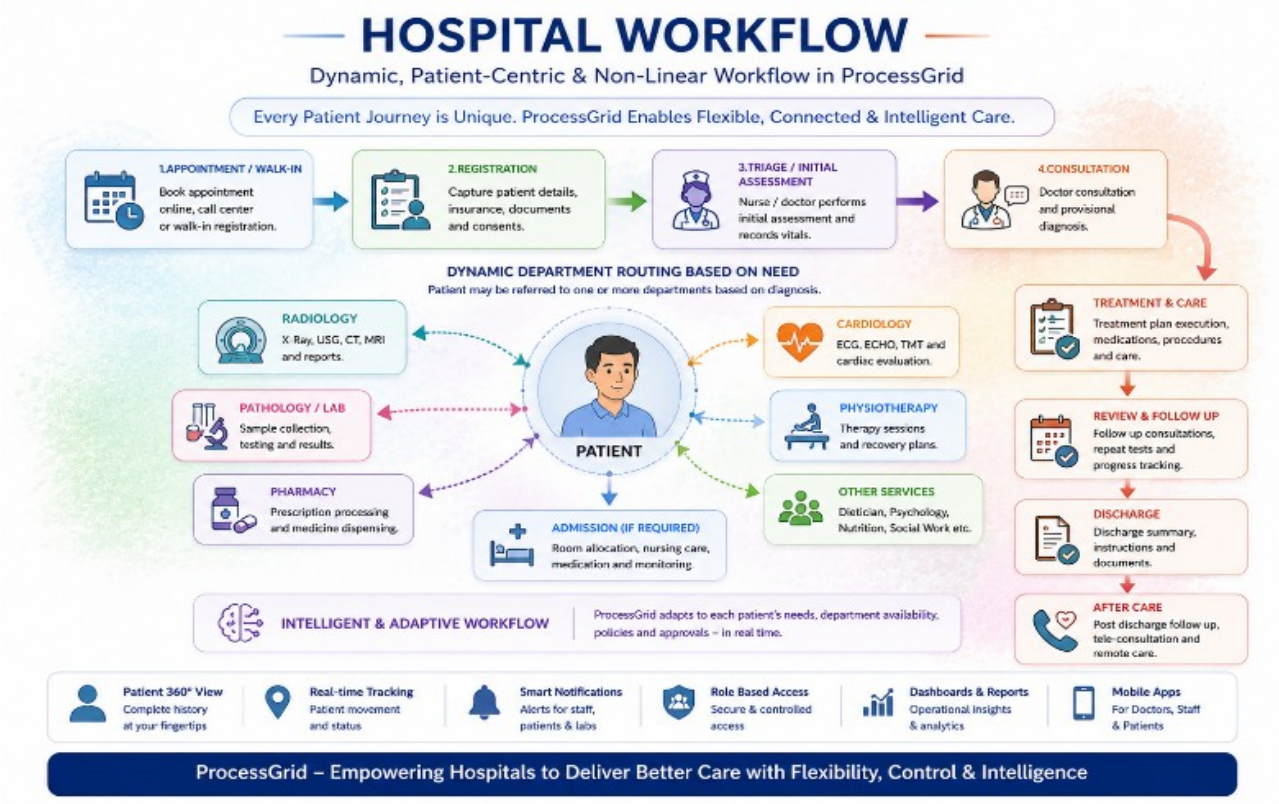
DPDP Complaint Hospital Management System



Hospital workflows are dynamic and patient-driven, where patients may move across multiple departments based on diagnosis, treatment requirements and medical decisions.

ProcessGrid enables hospitals to manage flexible “any process to any process” workflows without being restricted to fixed workflow structures.

Hospital Workflow Features

- Single Integrated Patient Visit Life Cycle Management
- Patient Consent Workflows for Data Sharing
- Record Access Log for
- Record Deletion Request management
- DPDP and HIPPA compliance-oriented architecture
- Configurable support for ICD-10, SNOMED CT, and other

Audit
- Ward management, Billing and Insurance integration
- Pharmacy Management

coding standards

The platform provides centralized visibility into patient movement, treatment progress, approvals and departmental coordination.

ProcessGrid ERP for Hospitals – Medical Information Security & Compliance Features

Patient Medical Record Management

- Centralized patient medical record management integrated with workflow-driven hospital operations.
- Support for structured diagnosis recording using internationally recognized medical coding systems.
- Configurable support for ICD-10, ICD-11, SNOMED CT, LOINC, CPT, and future coding standards.
- Diagnosis records maintained as part of patient care workflows and clinical follow-ups.

Sensitive Medical Information Protection

- Separation of operational data and sensitive clinical information.
- Sensitive medical notes are stored independently from routine information with workflow references.
- Designed for handling confidential information such as psychiatric notes, addiction history, HIV-related information, genetic information, and other restricted clinical data.
- Encryption applied before storage to reduce unauthorized data exposure risks.

Encryption of Sensitive Information

- AES-256-GCM authenticated encryption for sensitive medical data.
- Encryption keys managed separately from stored medical records.
- Protection against unauthorized database access to sensitive patient information.
- Tamper detection through authenticated encryption mechanisms.

Role-Based Access Control

- Fine-grained permission management for medical records access.
- Separate permissions for:
  - Diagnosis information access
  - Sensitive clinical information access
- Access can be controlled at workflow, process, user type, group, and user levels.
- Supports principle of least privilege by restricting access only to authorized personnel.

Medical Audit Trail

- Automatic logging of patient medical record access events.
- Audit records include:
  - User identification
  - Patient related process reference
  - Date and time of access
  - Action performed
  - Record type accessed

    - IP address information
- Provides accountability and traceability for sensitive medical data access.

Clinical Record Integrity

- Sensitive clinical notes configured as append-only records.
- Historical entries remain preserved.
- Corrections and updates are recorded as new entries instead of overwriting existing information.
- Helps maintain clinical history integrity and medico-legal defensibility.

Medical Coding Support

- Integrated diagnosis code management.
- Configurable medical code systems per hospital, process, workflow, or department.
- Supports:
    - Primary Diagnosis
    - Secondary Diagnosis
    - Comorbidity
    - Provisional Diagnosis
- Historical diagnosis snapshots preserved even if master code descriptions change later.

Compliance-Oriented Architecture

The medical information architecture has been designed to support compliance objectives commonly associated with:

- India Digital Personal Data Protection Act (DPDP Act, 2023)

- Health Insurance Portability and Accountability Act (HIPAA) security principles
- Information security best practices for healthcare organizations
- Data minimization and access control requirements
- Auditability and accountability requirements for sensitive personal data

Data Governance Features

- Segregation of operational and sensitive medical information.
- Access logging for sensitive patient records.
- Encryption of protected medical information.
- Controlled disclosure of sensitive patient data.
- Support for retention of historical medical information.
- Reduced risk of unauthorized internal access through permission-based controls.

Hospital Deployment Flexibility

Suitable for:

- Clinics
- Multi-specialty hospitals
- Day-care centres
- Diagnostic centres
- Specialty medical practices
- Telemedicine operations
- Healthcare service providers

DPDP Complaint Hospital Management System

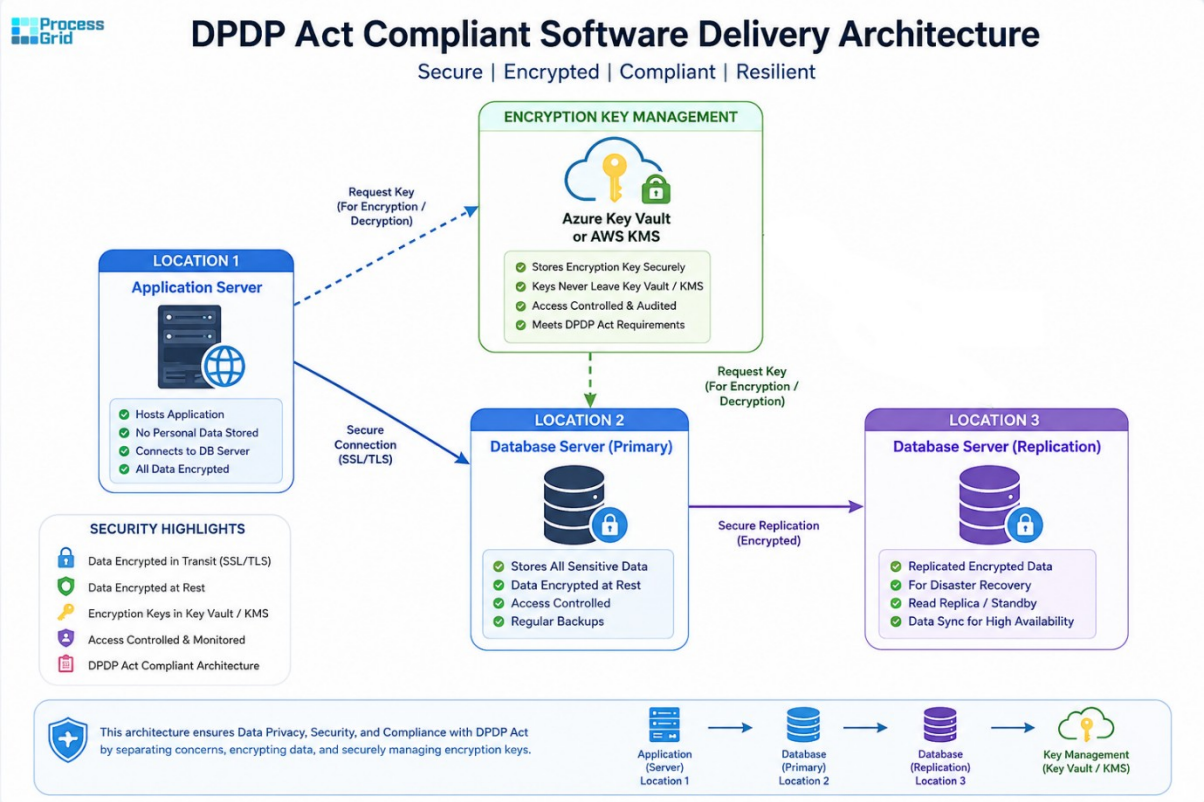
Current Medical Security Readiness

The platform currently includes:

- Diagnosis Management
- Medical Coding Support
- Sensitive Information Segregation
- AES-256-GCM Encryption (NIST Approved)
- Role-Based Permissions
- Patient Access Audit Trail
- Automatic Audit Logging
- Clinical History Preservation
- Workflow-Based Medical Data Controls

These capabilities provide a strong foundation for secure handling of patient information while supporting operational efficiency and compliance-focused healthcare workflows.

DPDP Complaint Hospital Management System



ProcessGrid helps hospitals improve operational efficiency, patient care coordination and service quality through intelligent workflow automation

DPDP Complaint Hospital Management System

Designed, Developed and Marketed By:
Innovative Matrix Softech Pvt Ltd
Phone: +91.**8919039916**
Email: Info@ProcessGrid.in
Web: www.ProcessGrid.in | www.InnovativeMatrix.in