**16. Data Protection Impact Assessment (DPIA)**

**16.1. DPIA Objective**

The evaluation assesses privacy risks of handling personal and sensitive health data while establishing methods for HIPAA, GDPR and Australian Privacy Act compliance.

**16.2. DPIA Process Overview**

|  |  |  |  |
| --- | --- | --- | --- |
| **Step Name** | **Details** | **Risk Level** | **Mitigation Priority** |
| Data Processing Overview | The system processes patient information consisting of MRI scans (DICOM format) and personal demographics together with medical histories and referral forms and diagnostic reports and billing records. The system enables secure web-based portal operations for all processing functions and information distribution. | High | High |
| Purpose of Processing | The system provides MRI diagnostic services and prepares medical reports efficiently while enabling remote consultations through a protected payment and billing management system | |  |  | | --- | --- | | Low |  | | Medium |
| Data Characteristics | The platform handles extremely sensitive health records that contain personally identifiable information (PII) and MRI image data as well as clinical notes and financial details. | High | High |
| |  |  | | --- | --- | | Stakeholders |  | | The system includes patients together with radiologists and MRI technicians and administrative staff and referring physicians and payment processors and regulatory authorities. | Medium | Medium |
| Data Flow Analysis | Users input patient information into the portal that leads to secure database and PACS storage before authorized personnel can access it to generate reports or billing records. | High | High |
| Risk Identification | Potential threats include unauthorized access, information leaks, weak encryption, insufficient anonymization, phishing attempts, and breaches of privacy legislation. | High | High |
| Risk Mitigation Measures | - The system uses AES-256 encryption for stored data and TLS 1.3 encryption for data transfers.  - Role-Based Access Control (RBAC) combined with Multi-Factor Authentication (MFA) must be implemented.  - A secure system must store encrypted audit logs of all activities performed within it.  - The system must perform regular penetration tests along with security audits. | High | High |
| Data Minimisation | Only necessary medical and operational information should be collected for data protection purposes while keeping personal and marketing-related details out of the system. | Medium | Medium |
| Consent and User Rights | The system requires patients to give explicit consent during registration followed by the option to view their information and make requests for updates or deletion or data export. | Medium | High |
| Data Retention Policy | The medical and administrative records must be preserved according to Australian legal requirements of seven years before becoming anonymous or facing complete destruction. | Medium | High |
| Data Breach Response Plan | Establish immediate protocols for breach detection followed by containment and investigation then notify affected persons within 72 hours and report incidents to proper authorities. | High | High |
| Third-Party Compliance | All external vendors must fulfill HIPAA and GDPR requirements through Data Processing Agreements (DPAs) that they must sign. | High | High |

The system reduces privacy risks through encryption technologies along with data minimization strategies and strong access controls and anonymization techniques. The system follows Privacy by Design principles which ensure ongoing compliance with privacy laws and data protection best practices through its architectural design.