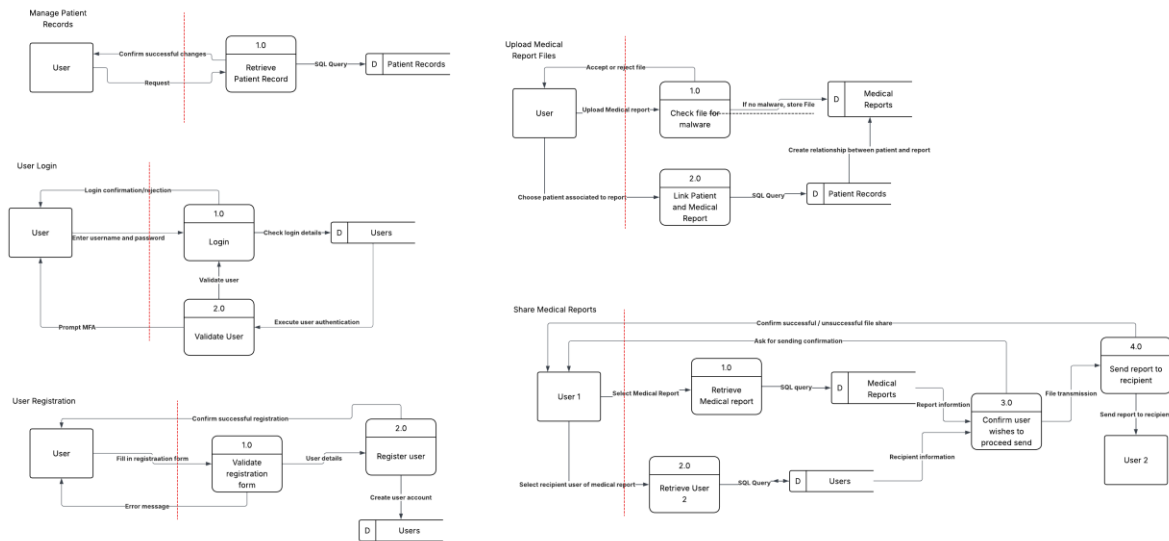


Threat Modelling & Risk Assessment

Data Flow Diagrams



Functional Requirements & Security Requirements

ID	Stage	Functional Requirements	Security Requirements
FR-01	User Authentication	System shall allow users to log in with username and password.	Passwords must be hashed, transmitted via HTTPS, and MFA required for admins
FR-02	User Registration	System shall allow users to register new accounts	Registration requires email verification and CAPTCHA
FR-03	Data Upload	User can upload a medical report file.	Files must be scanned for malware and restricted to .pdf/.docx formats
FR-04	Data Access	Healthcare professionals can view patient records	Only authorised roles can access records; all access logged
FR-05	Data Storage	System shall store health data in a database	Data must be encrypted at rest and backed up securely
FR-06	Data Modification	Healthcare professional can edit patient records	Data must be updated on the database
FR-07	Data Deletion	Healthcare professionals can delete patient records	Data must be removed from the database and any backups within 30 days
FR-08	Data Sharing	Healthcare professionals can share files and patient records with each other	Data must be encrypted before secure transmission via HTTPS to the recipient

STRIDE Threat Table & Risk Register

ID	Threat Addressed (STRIDE)	Description	Likelihood	Impact	Risk	Security Requirements
T-01	Spoofing / DoS	Attackers could impersonate health professionals or admins.	3	5	15 (High)	Enforce MFA, strong password policy, account lockout after failed attempts, device fingerprinting
T-02	Tampering	Attackers could modify patient medical records	2	5	10 (Medium)	Use HTTPS/TLS encryption, implement digital signatures and hash-based integrity checks to detect tampering
T-03	Repudiation	Users could deny action due to lack of audit logs	3	3	9 (Medium)	Use timestamps to maintain audit trails, use non-repudiation logs and store actions with immutable records
T-04	Information Disclosure	Sensitive patient data could get leaked due to an insecure database	2	5	10 (Medium)	Follow GDPR compliance, use secure API tokens, apply AES 256 encryption for data at rest, use TLS 1.3 for data in transit
T-05	Denial of Service	The user login form could get flooded with attempts, making the system	4	4	16 (High)	Implement CAPTCHA, IP throttling, and rate limiting, use traffic monitoring to

		unavailable to use				detect abnormal and frequent activity
T-06	Elevation of Privilege	Regular users could gain admin privileges by a buffer overflow	2	5	10 (Medium)	Enforce role-based access (RBAC), conduct regular privilege audits and apply principle of least privilege.

Mapping Security Requirements to GDPR and Compliance Needs

Security Requirement	Relevant GDPR Article or Compliance Need	Explanation
Encrypt user data	Art. 32 – Security of processing	Organisations must implement appropriate encryption and confidentiality measures.
Provide account deletion feature	Art. 17 – Right to erasure	Users can request that their data be deleted permanently.
Log user consent	Art. 7 – Conditions for consent	Consent must be explicit and auditable.
Restrict cross-border data transfers	Art. 44 – Data transfer restrictions	Data must stay within approved regions or have safeguards.
Notify breaches within 72 hours	Art. 33 – Breach notification	Organisations must report personal data breaches promptly.
Authenticate user attempting to login	Art. 32 – Security of Processing	Organisations must implement appropriate encryption and confidentiality measures.
Enforce access control policies	Art. 32 – Security of Processing	Organisations must implement appropriate encryption and confidentiality measures.