Security Analysis and Risk Assessment

(Based on the Medical Appointment & Records System schema)

This section provides a structured security analysis of the Medical Appointment & Records System. It focuses on identifying sensitive data, evaluating the risk of database actions, and identifying realistic security threats. This analysis forms the justification for the access control, encryption, and auditing mechanisms implemented in other parts of the project.

Data Sensitivity Classification

The database stores different categories of healthcare, personal, and financial data. Each table and column is classified according to the impact of unauthorized disclosure or modification, following healthcare data protection principles (e.g., GDPR).

Sensitivity Levels

- **High**: Medical or financial data whose exposure may cause legal, medical, or financial harm.
- **Medium**: Personally identifiable information (PII) with privacy impact.
- **Low**: Operational or system metadata with limited impact if exposed.

Data Sensitivity Classification Table

Table	Column	Sensitivity	Justification
users	username	Medium	Identifies system users
users	password_hash	**High**	Credential compromise risk
users	role	Medium	Role exposure enables targeted attacks
patients	full_name	Medium	Personally identifiable information
patients	dob	Medium	PII, identity profiling risk
patients	contact_info	Medium	Address and contact privacy risk
medical_records	diagnosis	**High**	Highly confidential medical information
medical_records	treatment_notes	**High**	Detailed private health data
medical_records	visit_date	Medium	Medical history inference
prescriptions	drug_name	Medium	Health-related information
prescriptions	dosage	**High**	Incorrect disclosure may cause physical harm
prescriptions	frequency	**High**	Medication misuse risk
billing	amount	Medium	Financial privacy
billing	insurance_provider	**High**	Insurance and financial fraud risk

Table	Column	Sensitivity	Justification
billing	insurance_claim_id	**High**	Insurance identity abuse risk
audit_logs	action	Low	System monitoring data
audit_logs	details	Medium	May expose operational behavior

This classification demonstrates that medical_records, prescriptions, and billing contain the most sensitive data and therefore require encryption, strict access control, and auditing.

Action Sensitivity Classification

Beyond data sensitivity, certain database actions pose significant risks when performed incorrectly or by unauthorized users. These actions are evaluated based on their potential impact on patient safety, privacy, and system integrity.

Action Sensitivity Table

Action	Risk Level	Explanation
Viewing medical records	**High**	Violates medical confidentiality
Updating diagnosis	**Critical**	Incorrect changes may lead to wrong treatment
Updating treatment notes	**Critical**	Directly affects patient care decisions
Creating prescriptions	**Critical**	Enables medication misuse
Updating prescription status	**High**	False dispensing records
Deleting appointments	Medium	Disrupts healthcare operations
Accessing billing data	**High**	Financial fraud and privacy risk
Modifying insurance details	**Critical**	Enables insurance abuse
Creating audit logs	Low	Operational integrity purpose

This analysis justifies:

- Column-level UPDATE restrictions
- Role separation between doctors, pharmacists, and administrators
- Prevention of DELETE operations on medical records

Threat Identification and Risk Analysis

Healthcare databases are high-value targets for both external attackers and insider threats. The following threats are considered realistic within the scope of this system.

Threat Identification Table

Threat	Description	Potential Impact	Mitigation Reference
Unauthorized access	External attacker gains DB access	Full data breach	RBAC & RLS
Role misuse	User accesses data outside their role	Privacy violation	Least-privilege roles
SQL injection	Malicious query manipulation	Data leakage or corruption	Restricted privileges
Insider threat	Authorized user abuses access	Silent data misuse	Auditing & logging
Backup theft	Stolen pg_dump backup	Complete database exposure	Backup encryption
Misconfigured privileges	Excessive GRANT permissions	Privilege escalation	Default access revocation
Privilege escalation	User gains admin-level access	System compromise	Role separation
Audit log tampering	Logs altered or deleted	Loss of accountability	Restricted audit access

These threats demonstrate that security must be enforced at multiple layers, including role-based access control, row-level security, encrypted storage, and audit logging.

Conclusion

This security analysis highlights the sensitivity of medical, prescription, and billing data within the Medical Appointment & Records System. By classifying data and actions and identifying realistic threats, this section provides the foundation for the security mechanisms implemented in subsequent parts of the project, including encryption, RBAC, row-level security, and secure backup handling.