Summary Report

Digital Security in Hospital Applications

Name: Nikhil Sandip Rokade

Organization: Heal Bharat

Date: 04-06-2025

---

1. Application Overview

The hospital web portal enables:

- Patients and doctors to log in
- View and manage appointments
- Access health records
- Communicate with 3rd-party APIs (e.g., labs, insurance)

However, it lacks essential security features like access control, encryption, and auditing.

---

2. Security Flaws Identified

No.	Flaw	Risk Category
1	No role-based access	Access Control
2	Public API endpoints	API Security
3	No HTTPS encryption	Data in Transit
4	Plain-text storage of patient data	Data at Rest
5	Weak passwords	Authentication
6	Sessions never expire	Session Management
7	No audit logging	Auditing
8	No backup strategy	Backup & Recovery
9	Phishing risk to staff	Social Engineering
10	Unsecured cloud storage	Cloud Security

---

3. Recommended Solutions

- TLS 1.2+ encryption for login/API
- Role-based access (RBAC) for patients/doctors/admins
- AES-256 encryption for data at rest
- OAuth 2.0 or API key gateway
- Strong password policies + 2FA
- Auto-logout sessions
- Audit logs for access control
- Encrypted daily backups
- Staff training & phishing simulation
- Secure cloud configuration

---

4. Compliance Overview

- **HIPAA (USA)**:
  - Requires access control, encryption, logging
  - HIPAA Security Rule
- **DISHA (India)**:
  - Mandates secure handling of electronic health info
  - DISHA Bill – India 2018
- **OWASP Top 10**:
  - Issues found match A3 (Data Exposure), A5 (Access Control)

---

5. Conclusion

The system poses serious risks to patient privacy and institutional compliance. Implementing strong access control, encryption, and logging can ensure trust and legal compliance.
