Security Audit Report: Hospital Web Application

Overview of the System

This report evaluates the digital security of a hospital web application. The system allows patients and doctors to log in, access health records, book appointments, and communicate via APIs with third-party services like insurance and pharmacies.

Identified Security Flaws

Serial Number	Security Flaw	Risk
1	Plain-text data storage	Patient data exposure if database is compromised
2	Weak password policy	Easy for attackers to guess or brute-force accounts

3	No 2FA	Increases risk of unauthorized account access
4	Public API with no authentication	Anyone can access patient data via the API
5	No data encryption in transit	Man-in-the-middle attacks on login or reports
6	Unrestricted admin panel access	Insider threats or external abuse
7	No logging of user actions	Undetected suspicious activity
8	No backup mechanism	Data loss from server failure or attack
9	Vulnerable third-party API	Insurance API could leak sensitive data
10	Insecure session management	Session hijacking risk on

		shared/public devices

Regulatory Compliance Notes

- **HIPAA (USA)** mandates encryption, user authentication, logging, and access controls for Protected Health Information (PHI).
- **DISHA (India)** enforces data privacy, consent-based access, and secure storage/processing of health records.
- Non-compliance may lead to legal penalties and data breach liability.

Recommended Security Solutions

Flaw	Recommended Fix
Plain-text storage	Use AES-256 encryption for data at rest
Weak passwords	Enforce strong password rules + expiry policy

No 2FA	Implement Two-Factor Authentication (OTP, TOTP)
Public API	Use OAuth2.0 + API Gateway with IP throttling
No encryption	Use HTTPS with TLS 1.2+
Admin access	Role-based access with session timeout
No Logs	Enable audit logging, review weekly
No backup	Schedule encrypted automatic backups
3rd-party APIs	Verify partners, use API token management
Sessions	Use secure cookies with expiration and logout

Conclusion

The hospital web application is vulnerable to multiple security risks. By following HIPAA/DISHA guidelines and implementing best practices like encryption, access control, and logging, the system can protect patient data effectively and ensure regulatory compliance.