Hospital Threat Checklist

Threat Category	Description	Present?	Mitigation Applied
Access Control	Unrestricted admin panel access	Yes	Role based action
Data Protection	Plain-text storage of patient info	Yes	AES encryption
Authentication	Weak or reused passwords	Yes	2FA
API Security	Unauthenticated API endpoints	Yes	API Gateway
Auditing	No logging of user activity	Yes	Enable logging
Backup & Recovery	No backups of patient database	Yes	Automated encrypted backup
Session Management	No session expiration or secure cookies	Yes	Secure Cookies
Encryption in Transit	HTTP used instead of HTTPS	Yes	TLS 1.2+
User Roles	Single role access for all users	Yes	Define Patient/Doctor/Admin
Third-Party Integration	Unverified insurance APIs	Yes	Partner audits, token-based control