# Hospital Risk Assessment Project:

## Step 1: Identify Assets:

Assets are valuable items the hospital must protect:  
- Electronic Health Records (EHR) system  
- Medical imaging devices (MRI, X-Ray machines connected to network)  
- Hospital Wi-Fi and VPN connections  
- Billing and payment processing system

## Step 2: Identify Threats:

Threats are anything that could harm the assets:  
- Ransomware attack (e.g., Scripps Health case)  
- Phishing attacks targeting staff  
- Insider misuse of patient data  
- Physical theft of laptops with patient data

## Step 3: Identify Vulnerabilities:

Vulnerabilities are weaknesses that could be exploited:  
- Legacy systems with outdated software  
- Lack of phishing awareness among staff  
- Patient data not encrypted on devices  
- Weak access controls with too many permissions

## Step 4: Identify Risks:

Risks are possible bad outcomes if threats exploit vulnerabilities:  
- Data breach from ransomware → HIPAA fines and lawsuits  
- Phishing attack → unauthorized access to records  
- Insider misuse → privacy violations  
- Lost laptop → data exposure and financial penalties

## Step 5: Risk Assessment:

Each risk is rated by Likelihood and Impact:  
- Ransomware attack → Likelihood: High | Impact: High  
- Phishing attack → Likelihood: High | Impact: Medium  
- Insider misuse → Likelihood: Medium | Impact: High  
- Lost laptop (unencrypted) → Likelihood: Medium | Impact: High

## Step 6: Apply Controls:

Controls reduce risks to an acceptable level:  
- Deploy endpoint protection and backups  
- Enforce Multi-Factor Authentication (MFA)  
- Encrypt patient data on all devices  
- Conduct regular phishing awareness training  
- Use role-based access control

## Step 7: Document Residual Risks:

Even after controls, some risk remains:  
- Ransomware may still cause downtime  
- Staff may still click phishing links  
- Insider misuse is possible but reduced with monitoring  
- Encrypted laptops may still be targeted for other reasons