Milestone 3

Attack Profile & Damage Assessment

1. Attack Vectors

These are the methods attackers could use to gain unauthorized access or disrupt the EHR system.

Vector	Description
Phishing	Attackers trick hospital staff into giving up credentials via fake emails or login pages.
Credential stuffing	Using leaked passwords from previous breaches to log in to hospital accounts.
Remote access abuse	Exploiting insecure VPNs or telehealth portals to access internal systems.
Software vulnerabilities	Exploiting unpatched EHR software or server-side weaknesses to gain unauthorized access.
Insider threat	Disgruntled or negligent employees misusing authorized access to cause damage or exfiltrate data.

2. Attacker Motivation & Capabilities

Threat Actor	Motivation	Capabilities
Cybercriminals	Financial gain via data theft, ransomware, or extortion.	Moderate to high (phishing kits, ransomware-as-a-service).
Hacktivists	Political or ethical motives, e.g., targeting health systems.	Moderate (DDoS tools, public exploits).
Insiders (malicious or negligent)	Revenge, bribery, or accidental misconfiguration.	High access level, often bypasses basic defenses.
Nation-state APTs	Surveillance or large-scale disruption (less likely here).	Advanced (zero-days, stealthy persistence).

3. Potential Damage Assessment (Scenarios in the other PDF)

Impact Area	Possible Damage from Successful Attack
Safety and Health	Delays or denial of patient care; potential harm or fatalities.
Confidentiality	Breach of sensitive health records (PHI); GDPR or HIPAA violations.
Availability	EHR downtime; clinical services halted.
Reputation and Trust	Public backlash, loss of patient trust, media coverage.
Financial and Legal	Regulatory fines, lawsuits, breach notification costs, ransom payments.
Academic & Research Loss	Interrupted or corrupted clinical trial data; loss of credibility and funding.

4. Recommended Countermeasures

Category	Control
Administrative	Phishing awareness training, insider threat reporting policies, role-based access reviews.
Technical	Email filtering, MFA, endpoint detection and response (EDR), VPN hardening, encryption of backups.
Physical	Locked server rooms, badge-based access to clinical IT areas, secure disposal of printed PHI.
Monitoring & Response	SIEM deployment, real-time alerts, regular incident response exercises.