Attack Profile and Potential Damage Assessment for the University Hospital EHR System

Introduction

The Electronic Health Record (EHR) system at the university hospital is a mission-critical platform that stores patient histories, clinical decisions, and diagnostic data. It is accessed by doctors, nurses, and administrative personnel across departments and locations. Due to its high sensitivity and regulatory constraints (HIPAA, GDPR), the EHR system is a prime target for a wide range of cyber threats. This assessment defines four high-risk attack vectors, analyzes attacker profiles, and simulates potential consequences based on real-world tactics.

List of Attack Vectors

1. Phishing and Credential Theft
2. Remote Access Exploitation (VPN Abuse)
3. Insider Threat
4. Ransomware via Software Vulnerabilities
5. Credential Stuffing

ATTACK PROFILE 1: Phishing and Credential Theft

1. Motivation & Capabilities of Potential Attackers

- Cybercriminals seek to harvest credentials for ransomware or extortion.
- Insider or negligent users may fall victim unknowingly, providing access to attackers.

- Attacks often rely on mass phishing campaigns using public kits or spoofed email domains.
- **Capability Level**: Low to Moderate — phishing can be executed even by unskilled actors.

---

2. Potential Damage Assessment

Best-Case Scenario

- **Date of Analysis**: April 23, 2025
- **Description**: A clinical staff member receives a phishing email, but due to awareness training, does not click the link and reports it to IT.
- **Scenario Risk**: Low
- **Scenario Cost**: Very low — only time lost to incident triage.
- **Scenario Probability of Spread**: Very low

Most Likely Scenario

- A staff member enters credentials into a spoofed page, but MFA blocks the login. Security detects foreign login attempt and locks the account.
- **Scenario Risk**: Moderate
- **Scenario Cost**: Low to moderate — credential resets, log analysis.
- **Scenario Probability of Spread**: Low

Worst-Case Scenario

- Multiple staff fall victim. Attacker gains access to EHR, exfiltrates records, and modifies files.
- **Scenario Risk**: High
- **Scenario Cost**: High — includes legal penalties, breach notification, and care disruption.
- **Scenario Probability of Spread**: Moderate

---

3. Recommended Countermeasures

- Mandatory MFA for all staff accounts
- Quarterly phishing simulations and awareness training

- Email filtering and spoofed domain detection
- Role-based access control with audit trails

ATTACK PROFILE 2: Remote Access Exploitation (VPN Abuse)

1. Motivation & Capabilities of Potential Attackers

- Remote access channels, if weakly secured, allow external attackers to pivot into internal systems.
- Telehealth systems and admin panels accessible over VPN may be improperly segmented.
- **Capability Level**: Moderate — often requires scanning for open services and credential reuse.

---

2. Potential Damage Assessment

Best-Case Scenario

- Attack attempt blocked by VPN hardening and connection throttling; IP is blacklisted.
- **Scenario Risk**: Low
- **Scenario Cost**: Minimal – threat contained before access
- **Scenario Probability of Spread**: Very low

Most Likely Scenario

- Attacker reuses staff credentials to access internal dashboard, but is blocked by MFA and restricted network zones.
- **Scenario Risk**: Moderate
- **Scenario Cost**: Moderate — investigation and access review required
- **Scenario Probability of Spread**: Low to Moderate

Worst-Case Scenario

- Attacker gains VPN access, laterally moves to EHR system, disables backups, encrypts systems.
- **Scenario Risk**: High

- **Scenario Cost**: High to Critical — downtime, recovery, ransom, legal liabilities
- **Scenario Probability of Spread**: High

---

3. Recommended Countermeasures

- Harden VPN with MFA and IP-based access control
- Log and monitor all remote access sessions
- Implement jump-boxes for remote admins
- Conduct regular credential rotation and access reviews

ATTACK PROFILE 3: Insider Threat

1. Motivation & Capabilities of Potential Attackers

- Disgruntled staff or negligent insiders may intentionally or accidentally cause harm.
- High-privilege access allows data exfiltration, alteration, or deletion.
- **Capability Level**: High — insiders already have authorized access.

---

2. Potential Damage Assessment

Best-Case Scenario

- Misuse attempt is caught by real-time alerting or DLP controls; action blocked.
- **Scenario Risk**: Low
- **Scenario Cost**: Very low — internal report only
- **Scenario Probability of Spread**: Very low

Most Likely Scenario

- Staff accesses records without authorization. Access logs flag the activity and disciplinary action is taken.
- **Scenario Risk**: Moderate
- **Scenario Cost**: Moderate — HR intervention and potential patient complaint

- **Scenario Probability of Spread**: Low

Worst-Case Scenario

- Insider exports a patient database and shares it externally. Legal inquiry is launched, and hospital reputation is severely damaged.
- **Scenario Risk**: High
- **Scenario Cost**: High — fines, lawsuits, investigation, and public trust erosion
- **Scenario Probability of Spread**: Moderate

---

3. Recommended Countermeasures

- Enforce role-based access control
- Monitor audit logs and alert on unusual data exports
- Conduct insider threat awareness and ethics training
- Segregate duties for sensitive roles

ATTACK PROFILE 4: Ransomware via Software Vulnerabilities

1. Motivation & Capabilities of Potential Attackers

- Attackers exploit unpatched EHR system components or remote code execution bugs.
- This vector is frequently used by financially motivated ransomware groups.
- **Capability Level**: Moderate to High — requires scanning, exploit crafting, and payload deployment.

---

2. Potential Damage Assessment

Best-Case Scenario

- The vulnerability is blocked by EDR or patched before exploitation; alerts are raised.
- **Scenario Risk**: Low
- **Scenario Cost**: Minimal — patching and incident verification only

- **Scenario Probability of Spread**: Very low

Most Likely Scenario

- A low-impact component is exploited, but antivirus quarantines the payload before full execution.
- **Scenario Risk**: Moderate
- **Scenario Cost**: Moderate — cleanup, system scans, downtime on a few machines
- **Scenario Probability of Spread**: Low

Worst-Case Scenario

- Vulnerability leads to full ransomware deployment; EHR files are encrypted, backups compromised, care operations disrupted.
- **Scenario Risk**: Critical
- **Scenario Cost**: Severe — ransom negotiation, forensic analysis, full system rebuild
- **Scenario Probability of Spread**: High

---

3. Recommended Countermeasures

- Patch management policy and routine vulnerability scanning
- Endpoint Detection and Response (EDR) tools with behavior-based protection
- Network segmentation between frontend and backend systems
- Offline, immutable backups with test restores

ATTACK PROFILE 5: Credential Stuffing

1. Motivation & Capabilities of Potential Attackers

- Attackers use previously leaked credentials (from unrelated breaches) to gain unauthorized access to hospital systems.
- Healthcare staff may reuse personal or weak passwords across multiple systems, making this vector effective.

- **Capability Level**: Low to Moderate — requires automated tools and access to breached credential databases.

---

2. Potential Damage Assessment

Best-Case Scenario

- Login attempts are blocked by lockout policies and MFA; IP is blacklisted.
- **Scenario Risk**: Low
- **Scenario Cost**: Very low — security logs reviewed, no breach.
- **Scenario Probability of Spread**: Very low

Most Likely Scenario

- Staff credentials are reused on the EHR login. MFA blocks access, but attacker learns usernames and escalates to phishing.
- **Scenario Risk**: Moderate
- **Scenario Cost**: Low to moderate — login resets, user awareness follow-up.
- **Scenario Probability of Spread**: Low

Worst-Case Scenario

- Attacker successfully logs into multiple accounts using reused passwords, gains unauthorized access to EHR and internal communications.
- **Scenario Risk**: High
- **Scenario Cost**: High — patient record leakage, privacy breach notifications, internal audit.
- **Scenario Probability of Spread**: Moderate

---

3. Recommended Countermeasures

- Enforce password complexity and rotation policies
- Implement MFA across all user-facing systems
- Monitor for anomalous login behavior (geo-impossible logins, login velocity)
- Conduct staff training on password hygiene and credential reuse risks