# Medical Clinic Network Security Report

## *1. Basic Analysis of the Attack Surface*

### 1.1 Endpoints and Devices:

- **Types of Devices Present:**
  - Servers for patient health records storage (EHR system on Ubuntu)
  - Front desk workstations (Windows desktop computers)
  - Digital X-ray sensors and imaging devices
  - Point-of-sale (POS) terminals
  - Wireless access points (WPA2 encrypted)
- **Patch and Update Status:**
  - Patching is done manually once a month by front desk staff.
  - Confirmation could be achieved through centralized patch management software or automated vulnerability scans.

### 1.2 Network Layer:

- **IP Address Ranges:**
  - Internal: 192.168.0.0/24
  - External:
    - SoHo: 139.60.168.191
    - Midtown: 139.177.192.141
    - Park Slope: 139.48.0.109
- **Exposed Network Services/Open Ports:**
  - Regular scans and firewall configurations can help identify exposed services and open ports.

### 1.3 Web Applications:

- **Public-Facing Applications:**
  - Web interface for EHR and billing systems accessible on premises.
- **Technologies Used:**
  - EHR hosted on Ubuntu, cloud backups via HTTPS.

### 1.4 User Accounts and Authentication:

- **User Account Management:**
  - Front desk endpoints use Office 365 accounts.

    - EHR system uses one shared account with full privileges, stored in 1Password.
- **Password Security:**
    - Need assessment for weak/default passwords.
    - Multi-factor authentication (MFA) is not mentioned, should be implemented.

### 1.5 Data Exposure:

- **Sensitive Data Handling:**
    - Patient records, treatment plans, and images.
    - Data encrypted at rest and in transit (EHR and imaging systems).
- **Data Protection Measures:**
    - Encrypted backups to AWS.
    - Regular manual updates and cloud synchronization.

### 1.6 Cloud Services:

- **Cloud Services in Use:**
    - AWS for backups and imaging data storage (S3 buckets, EC2 for scripts).
- **Service Models:**
    - SaaS for EHR backups, cloud-managed SIEM and EDR.

### 1.7 Patch Management:

- **Handling and Process:**
    - Manual patching once a month with calendar reminders.
    - EDR performs weekly vulnerability scans.