Computer Forensics and Security BS (hons) 2nd year

Will Gusackova
28/04/2025

Security Requirements and Threat Analysis of the EPIC EHR System

Abstract of Report:

This report examines the EPIC electronic health records (EHR) system, specifically focusing on its security requirements and potential vulnerabilities. Using personal experience with the EPIC system at the Cleveland Clinic in Ohio from employment at RelateCare, as well as research into known issues and threats, the report explores both functional and misuse cases to identify and mitigate risks. Using threat modeling and misuse case analysis, the report proposes security-focused requirements and recommendations aimed at enhancing the system's resilience against both internal and external attacks.

Introduction to EPIC Electronic Health Records (EHR) System:

EPIC is an electronic health records (EHR) system used widely across the world, most prominently in the United States. It is designed to manage and store medical information such as appointment scheduling, cancellations, waiting lists, and patient history, helping healthcare providers deliver accurate and timely care.

The system contains highly sensitive patient data, including PPSN numbers, insurance details, names, ages, genders, phone numbers, addresses, medical histories, and any disabilities or special needs. This information is accessible to a range of authorized users, including doctors, nurses, receptionists, and administrative staff, depending on their role.

EPIC supports critical healthcare functions by improving communication between departments, reducing manual errors, and streamlining administrative workflows. Due to the nature of the data it handles, security and privacy are essential, particularly in ensuring compliance with healthcare regulations such as HIPAA in the United States, which all employees must agree to the terms and conditions, breaches are delt through legal consequences. Due to the complexity of the system and the sensitivity of the data it handles, proper training is essential to ensure that staff use EPIC effectively and securely. To avoid costly mistakes or data breaches, employees must be trained to recognize phishing attacks and follow established security protocols.

However, like many complex systems, EPIC is potentially vulnerable to security threats, including unauthorized access, insider misuse, and data breaches. These risks make it necessary to thoroughly analyze its requirements from a security perspective and implement strong protections at every stage of development.

User Roles and Access Overview:

The EPIC EHR system involves four main user roles: **Administrator**, **Employee (Booking Agent/Receptionist)**, **Doctor**, and **Patient**. Each role has specific responsibilities and system access, with permissions governed by HIPAA compliance and departmental boundaries.

Administrator:

- Responsible for creating, managing, and revoking accounts for employees and doctors.
- Can assign access based on departmental roles and responsibilities.
- Has administrative privileges over system configurations, permissions, and security settings.
- Can monitor user activity and conduct audits to ensure compliance with security policies.

Employee (Booking Agent / Receptionist):

- Serves as the primary point of contact for patients, typically over the phone.
- Must verify **three to four pieces of personal information** (e.g., date of birth, address, insurance number) before accessing or disclosing any patient information.
- If the patient fails to provide correct information, the employee is prohibited from proceeding with the request or sharing any data.
- Upon successful verification, employees may:
    - Book or cancel doctor appointments on behalf of the patient.
    - Add the patient to relevant departmental waiting lists.
    - Update some clinical details such as contact information.

Doctor:

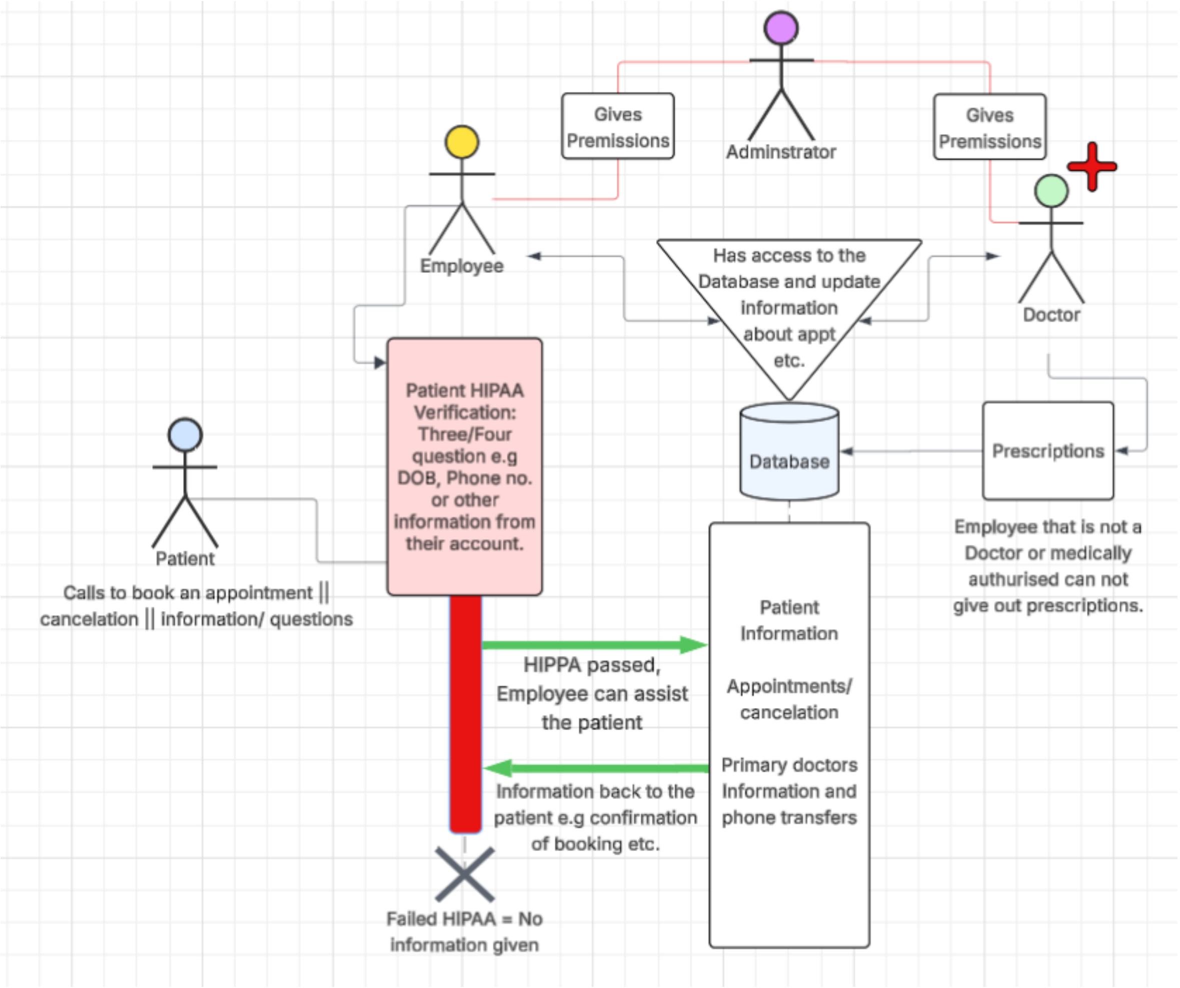
- Has access to clinical data for patients within their assigned department.
- Can view and update patient medical records, add clinical notes, and review test results.
- Authorized to prescribe medication and electronically send prescriptions to pharmacies.
- Access is restricted to their specific department to maintain confidentiality and minimize unnecessary exposure to unrelated records.

Patient

- Patients do not have direct access to the EPIC system.
- They may call the clinic to request information or schedule appointments.
- Identity verification is mandatory before any action can be taken on their behalf.

- All interactions must be mediated through a verified employee; patients cannot independently retrieve or update any data within the system.

Use-case diagram:

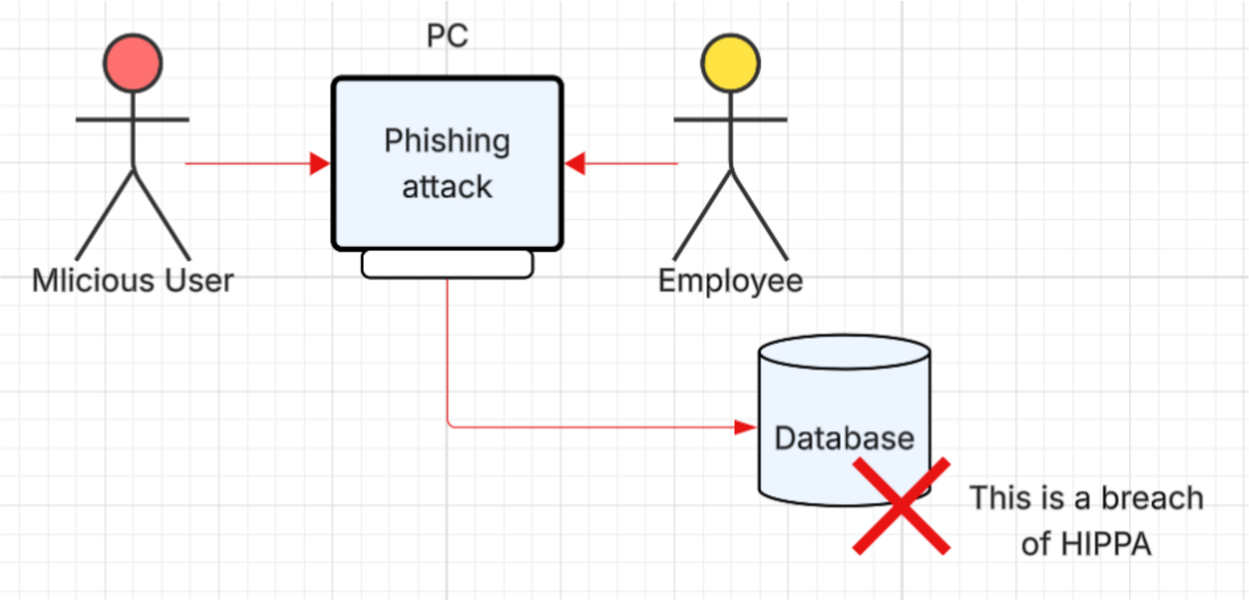

Gives Premissions
Adminstrator
Gives Premissions
Employee
Has access to the Database and update information about appt etc.
Doctor
Patient HIPAA Verification: Three/Four question e.g DOB, Phone no. or other information from their account.
Database
Prescriptions
Patient
Calls to book an appointment || cancelation || information/ questions
Employee that is not a Doctor or medically authurised can not give out prescriptions.
Patient Information
Appointments/ cancelation
Primary doctors Information and phone transfers
HIPPA passed, Employee can assist the patient
Information back to the patient e.g confirmation of booking etc.
Failed HIPAA = No information given

Unauthorized Access via Compromised Employee Account:

- **Actor (Threat Agent):** External Attacker or Insider
- **Goal:** Gain unauthorized access to patient records or system functions

  Scenario:
  An attacker gains access to a booking agents or doctor's account due to weak password practices, shared login credentials, lack of multi-factor authentication or an email phishing attack. Once inside, the attacker can view patient data, alter medical records, or download sensitive information without detection.

- **Impact:**
  - Exposure of large volumes of sensitive health information
  - Manipulation of medical records or prescriptions
  - Loss of trust in the system
  - Possible ransomware infection or data destruction



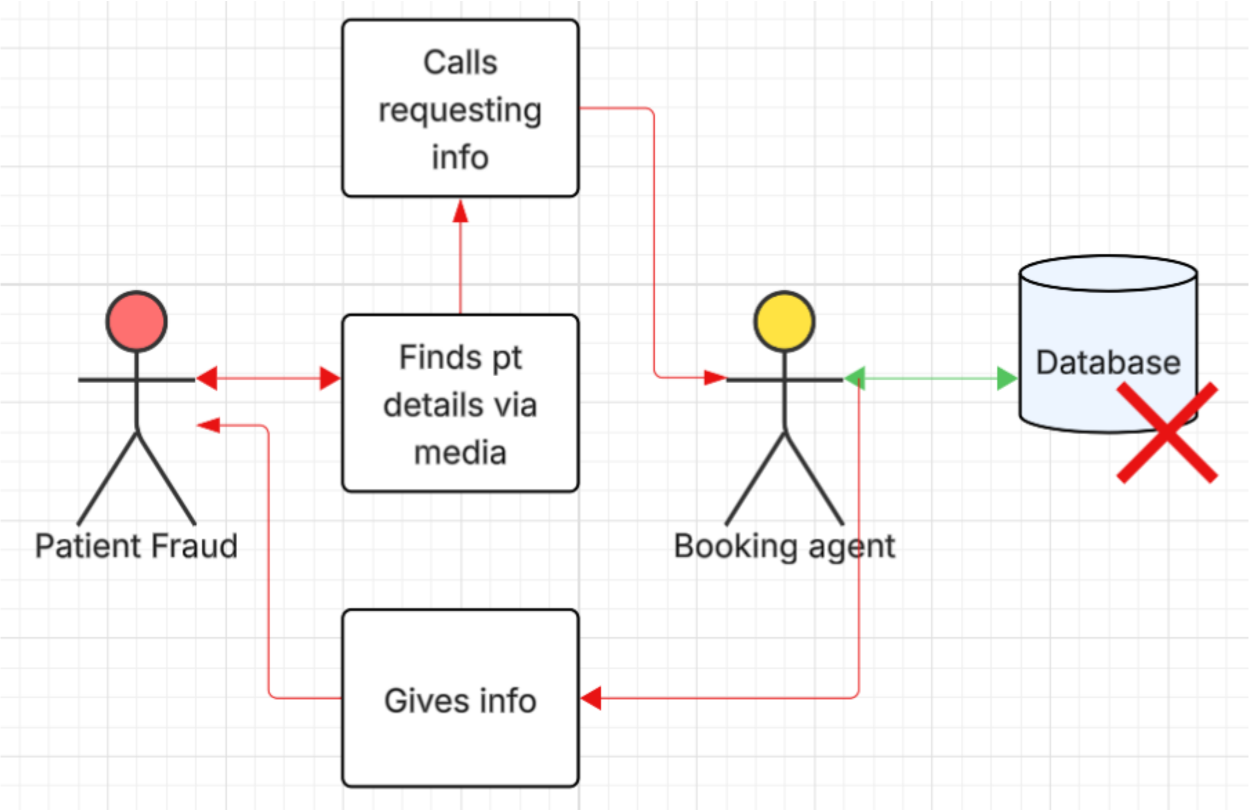
Social Engineering via Phone Call:

- **Actor (Threat Agent):** External Attacker (posing as a patient)
- **Goal:** Gain access to personal or medical information

  Scenario:
  The attacker calls the clinic pretending to be a patient. They attempt to answer the identity verification questions by guessing or using previously stolen information (e.g., from social media or data breaches). If the booking agent fails to properly verify the caller's identity or skips questions under pressure, the attacker may be given access to confidential information or allowed to make unauthorized appointment changes.

- **Impact:**
  - Breach of confidentiality

- Violation of HIPAA regulations
- Legal and financial repercussions for the clinic
- Potential for identity theft or further targeted attacks

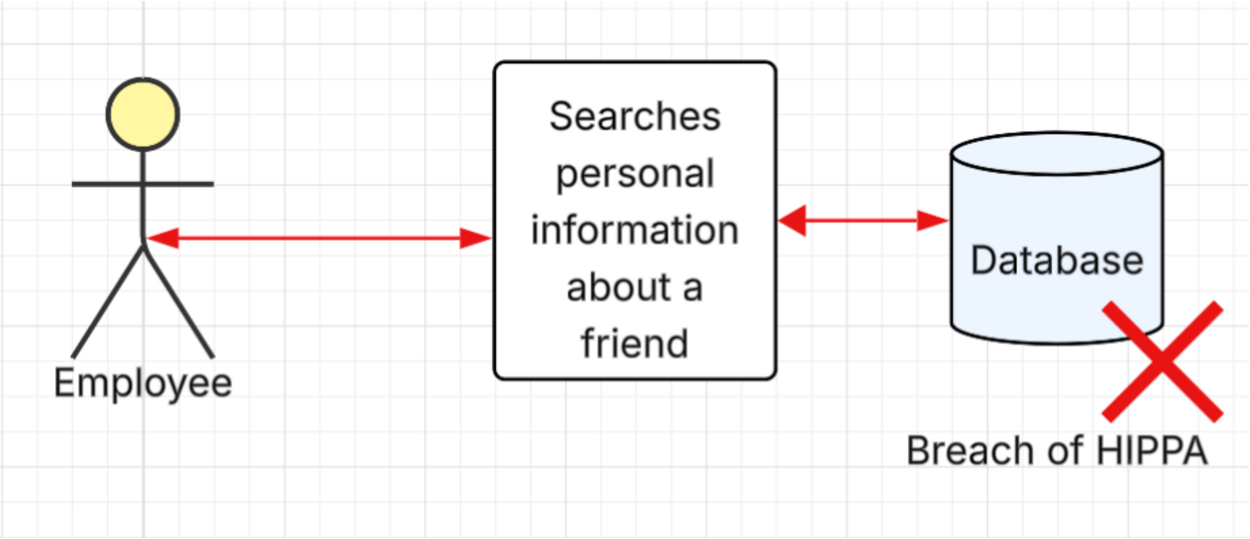


Insider Misuse of Access Rights:

- **Actor (Threat Agent):** Malicious or careless employee
- **Goal:** Access or misuse patient data outside their role

  Scenario:
  A receptionist or employee uses their access to look up information about a family member, public figure, or for personal curiosity—without a valid reason. This is especially dangerous if the system does not enforce departmental access limits or audit logs aren't reviewed regularly.

- **Impact:**
  - Breach of patient privacy
  - Disciplinary/legal action against staff
  - Regulatory fines for non-compliance
  - Need for incident response and patient notification



Augmented requirements:

In response to the identified misuse cases and potential vulnerabilities in the EPIC system, the following additional security requirements and mitigations are proposed.

Mandatory Security Training and Contracts

- All employees must undergo formal training in patient data protection, phishing awareness, and system usage before gaining access to EPIC.
- Employees are required to sign contracts acknowledging their responsibility to comply with HIPAA regulations and internal data security policies.
- Sharing patient information with unauthorized individuals is strictly prohibited and will result in disciplinary action.

Secure Network Connectivity

- All workstations connected to the EPIC system must use **wired Ethernet connections** to reduce the risk of interception through wireless vulnerabilities.
- Wireless access points must be disabled or restricted in areas where EPIC is in use unless secured with WPA3 encryption and MAC address filtering.
- Firewalls and network segmentation should be implemented to separate sensitive health data traffic from general internet use.

Multi-Factor Authentication (MFA)

- MFA is mandatory for all system logins, including:
    - **EPIC System Account**
    - **Virtual Machine Environment**
    - **Work Email Account**
- Each account must use a **unique, strong password** and a second factor (e.g., hardware token, app-based code, or smart card).
- Password reuse across systems is strictly prohibited to reduce the risk of credential stuffing or lateral movement in case of a breach.

System Performance & Reliability

- A stable and fast internet connection is required to ensure uninterrupted access to the EPIC system and reduce the chance of session timeout errors that may affect clinical operations.
- Downtime monitoring and fallback procedures (e.g., local backups or offline access protocols) should be in place in the event of network issues.

Recommendations and Test Plans:

To enhance the security, reliability, and auditability of the EPIC EHR system, the following recommendations and test plans are proposed. These are based on the identified misuse cases, system vulnerabilities, and standard industry best practices.

Recommendations:

Enforce Strict Role-Based Access Control (RBAC)

Access to system functions and patient data should be strictly governed by user roles. Doctors, employees, and administrators must only access information and features essential to their duties. Departmental access boundaries should be enforced to prevent unauthorized cross-departmental data viewing.

Implement Ongoing Security Training

All employees must receive mandatory, recurring training focused on:

- HIPAA compliance and data privacy
- Recognizing and reporting phishing and social engineering attempts

- Secure use of EPIC, including proper verification protocols
  Training should be updated yearly and tracked through an internal learning management system.

Enforce Multi-Factor Authentication Across All Accounts

Ensure MFA is enabled for all three core systems: the EPIC system, virtual machine environment, and work email accounts. Each should require unique credentials, and MFA tokens should be securely managed (e.g., hardware tokens or app-based authenticators).

Use Wired Network Connections and Network Segmentation

All systems accessing EPIC must use secured Ethernet connections rather than Wi-Fi to reduce the risk of man-in-the-middle attacks. Network segmentation should be applied to isolate sensitive clinical systems from general internet traffic.

Centralized Logging and Auditing

All user activity must be logged, including logins, data access, and record modifications. Logs should be reviewed regularly, stored securely, and integrated with an automated alert system to flag suspicious behavior.

Regular System Updates and Vulnerability Scanning

EPIC and all related software (including the VM and network infrastructure) must be updated regularly. Automated vulnerability scans and patch management tools should be used to detect and remediate security weaknesses.

Incident Response Plan

Develop and maintain an incident response plan, including steps for data breach notification, containment, and recovery. Staff must be trained on their responsibilities in case of a suspected breach.

Test Plans:

To validate the security posture of the EPIC system, the following test strategies are recommended:

Authentication & Authorization Testing

- Attempt to log in with invalid credentials or without MFA to confirm enforcement.
- Attempt access to unauthorized features based on role (e.g., receptionist trying to view patient diagnoses).

Social Engineering Simulation

- Conduct periodic phishing simulations to test employee vigilance.
- Simulate phone-based social engineering attacks to assess how well staff follow identity verification protocols.

Access Control and Boundary Testing

- Test for role-based access boundary enforcement (e.g., can a doctor in one department access another department's data?).
- Validate system behavior when a user account is terminated or disabled.

Encryption & Data Transmission Testing

- Confirm that all communications are encrypted using secure protocols (TLS 1.3).
- Test data storage encryption for backups and archived patient records.

Logging and Audit Trail Verification

- Attempt to access or modify patient data and verify that all actions are logged.
- Ensure logs capture user ID, timestamp, action, and affected records.

Penetration Testing

- Engage an external cybersecurity firm to conduct annual penetration tests, including network, application, and physical access assessments.

Performance and Failover Testing

- Test system behavior during high traffic (e.g., appointment rush) to verify connection speed and reliability.
- Simulate a network outage and test fallback or recovery procedures (e.g., paper-based backups or local cache access).

References:

Duo Security, 2024. *Duo Authentication for Epic*. [online] Available at: https://duo.com/docs/epic [Accessed 29 April 2025].

Duo Security, 2024. *Duo MFA Secures Epic Hyperdrive Against Cyber Threats*. [online] Available at: https://duo.com/blog/cisco-secure-access-by-duo-mfa-secures-epic-hyperdrive-against-cyber-threats [Accessed 29 April 2025].

Elation Health, 2024. *Cloud-Based EHR Security: 7 Tips You Need to Know*. [online] Available at: https://www.elationhealth.com/resources/blogs/tips-for-cloud-based-ehr-security [Accessed 29 April 2025].

Rublon, 2024. *Secure Electronic Health Records (EHR) with Rublon MFA*. [online] Available at: https://rublon.com/use-cases/healthcare-secure-ehr-access-mfa/ [Accessed 30 April 2025].

Rublon, 2024. *Enhance HIPAA Compliance with MFA for Healthcare*. [online] Available at: https://rublon.com/use-cases/hipaa-compliance-mfa-healthcare/ [Accessed 1 May 2025].

Vanderbilt University Medical Center, 2017. *Multi-factor Authentication to Enable E-Prescribing of Controlled Substances*. [online] Available at: https://news.vumc.org/2017/08/17/multi-factor-authentication-to-enable-e-prescribing-of-controlled-substances/ [Accessed 4 May 2025].

Wired, 2023. *Your Medical Data Is Code Blue*. [online] Available at: https://www.wired.com/story/plaintext-our-medical-security-is-code-blue [Accessed 4 May 2025].