EGERTON UNIVERSITY

COMP 437 ASSIGNMENT 15/02/2023

MEMBERS

1. **Mayaka Caleb Ombogo – S13/02627/20**
2. **Kipkosgei Kelvin Sanga – S13/02613/20**

Draft a security policy for protecting personal medical records kept on a computer system. Your policy should the access requirements patients, doctors and administrators

Introduction

A security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it. Good policy protects not only information and systems, but also individual employees and the organization as a whole. This security policy outlines the measures and protocols to be implemented for safeguarding personal medical records stored within the computer system of the hospital. It will outline all the steps to be taken in order to deter the attackers from being able to infiltrate the system and steal, alter and sabotage.

The following measures will be used to keep the system safe and secure:

1. Authentication

This is the process of verifying the identity of users before they are given access to a system or a particular resource in the system.

All the users in the system, patients, doctors and admins will be able to create accounts. On creating the accounts, they will be required to activate the account by clicking on a link sent to their email address.

To log in to the system, the users will use their email address or username and password.

Multi-Factor Authentication (MFA): When logging in to the system a SMS code will be sent to the user's phone number to verify of their identity.

Password Reset - All the uses will be able to reset their passwords if they forget. A reset link will be sent to their inboxes.

Biometrics identification - to make it easy for patients to quickly and securely log in, biometrics will be incorporated enabling them to us fingerprints to verify their identity

2. Access Control

This will be able to define the privileges and permission users have in the system. Doctors, administrator and patients will all have different access permission in the system.

The Role-Based Access Control (RBAC) - RBAC will be implemented to assign specific permissions based on user roles to ensure appropriate access levels. Doctors will be able to report to work, report out of work, add patients treated and other permissions The administrator will be able to access all these privileges from all user types. Patients will be able to book appointments with doctors and other services.

3. Business Continuity Plan

Regular Backups – The system will Maintain regular backups of medical records to ensure data integrity and availability in the event of system failures, disasters, or cyber-attacks. The backups should be stored at a separate location from the system. Preferably the cloud.

4. Data Encryption

Medical records and Data to be stored and transmitted will be encrypted using strong encryption algorithms to protect against unauthorized access and ensure confidentiality. Algorithms such as AES are to be used.

The system will employ secure communication protocols (e.g., SSL/TLS) for transmitting sensitive data over networks to prevent interception or eavesdropping. Https protocol will be used when the system is deployed.

5. Physical Security

Access Control Mechanisms – This will Restrict physical access to the computer rooms with servers and storage devices containing medical records through measures such as biometric locks, access cards, and surveillance systems. These locations should only be accessed by system administrators and other high-ranking officials.

Employing security guards -these guards are very important in preventing physical brute force and break-ins by physically being present at the site haven this will prevent unauthorized entry, theft, or damage.

Room Reinforcement – the server room doors, windows, and the ceiling will be reinforced with grilles to prevent break-ins.

6. System Decentralization

Migrating to a Distributed Architecture – The system will Implement a distributed system architecture to decentralize data storage and processing, reducing the risk of a single point of failure or large-scale data breaches. This is due to the fact that distributed systems are very fault tolerant, one fault cannot bring down the whole hospital system.

Redundancy – This can be confused with backups but it is essentially the act of distributing copies of medical records across multiple servers or locations to ensure redundancy and resilience against system failures or attacks. If one part of the system fails another one is available to pick up. This actually very important considering this is a critical system.

6. Antivirus and Antimalware

This is the use of antiviruses to identify and delete any possible malware that could be injected to the system.

Regular Updates to the system – The developers will be always patching any vulnerabilities that arise in the technologies used to build the system.

Scheduled Scans: All computers in the hospital running the system should have antivirus systems that are paid for and are capable of regular scans to detect any malware hiding in the pc that could possibly provide attackers with backdoors or monitor user keystrokes.

7. Compliance and Monitoring

Audit checks: We will Regularly audit the system to ensure compliance with relevant regulations and ensure that there are vulnerabilities.

Logging and Monitoring: The system will have logging and monitoring mechanisms to track user activities, detect suspicious behavior, and investigate security incidents promptly. In case there is an issue with the systems the log files will be a good starting point for the developers to debug the system and investigate.

Regular Reviews: we will regularly review and update the security policy to address emerging threats, technological advancements, and changes in regulatory requirements.

8. Training and Awareness

We will Provide ongoing training and awareness programs for users to educate the hospital team about security best practices and their responsibilities in protecting personal medical records. This step will take a significant amount of time since ignorance is one of the weakest links in computer security.