

Healthcare Management System

(MediCare Solutions)

(ACCA7028)

Group: 2

Group member:

- | | |
|-------------------------------|------------------|
| 1. Ms Janki Patel | (2520611) |
| 2. Mr Nirav Thummar | (2537379) |
| 3. Mr Dhaval Rami | (2528086) |
| 4. Mr Sameer Sukhadiya | (2536690) |

Introduction

MediCare Solutions is a healthcare organization that uses an Electronic Health Records (EHR) system to manage patient information, appointments, prescriptions, and treatment records.

Healthcare organizations handle highly sensitive information. Therefore, protecting patient data from cyber threats is essential to ensure privacy, trust, and uninterrupted healthcare services.

Objectives

- Identify security threats
- Analyse their impact
- Determine affected security principles
- Recommend security controls

Real-World Example

Example: NHS WannaCry Ransomware Attack (UK)

In 2017, the UK's National Health Service (NHS) was attacked by WannaCry ransomware.

Impact:

- More than 19,000 appointments cancelled
- Patient records became inaccessible
- Hospitals faced operational disruption
- Millions of pounds in losses

Lesson Learned:

Healthcare systems are major targets for cybercriminals.

Key Assets to Protect

Critical Assets

Patient Information

- Medical histories
- Lab reports
- Prescriptions

Healthcare Systems

- EHR Database
- Appointment Systems
- Staff Accounts

Infrastructure

- Servers
- Networks
- Backup Systems

Internal Threats

Internal Threats

Unauthorized Employee Access

Example:

A staff member accesses a celebrity's medical records without permission.

Security Principles Affected:

Confidentiality

Accountability

Consequences:

- Privacy violation
- Legal penalties
- Loss of public trust

External Threats

Phishing Attack

Example:

An employee receives an email pretending to be from IT Support.

The employee clicks the link and enters login credentials.

Impact:

- Stolen passwords
- Unauthorized access
- Data breaches

Security Principles Affected:

Confidentiality

Integrity

Ransomware Attack

Ransomware

Example:

Hackers encrypt all patient records and demand payment.

Consequences:

Hospital operations stop

Patient treatment delayed

Financial loss

Reputation damage

Risk Level:

Very High

SQL Injection Attack

SQL Injection

Example:

A hacker enters malicious code into the login page:

' OR '1'='1

Result:

- Access to patient database
- Data theft
- Data modification

Security Principles Affected:

Confidentiality

Integrity

Incidental Threats

Accidental Threats

Human Error

Example:

Wrong patient information entered.

Hardware Failure

Example:

Server crashes unexpectedly.

Natural Disaster

Example:

Flood damages hospital data center.

Impact:

- Data loss
- System downtime
- Delayed healthcare services

Security Principles

Confidentiality

Protect patient privacy.

Integrity

Ensure information remains accurate.

Availability

Ensure systems are always accessible.

Non-Repudiation

Prevent denial of actions performed.

Accountability

Track user activities.

Risk Matrix

Threat	Risk Level
Ransomware	High
Phishing	High
Insider Threat	High
SQL Injection	Medium-High
Hardware Failure	Medium
Human Error	Medium

Recommended Controls

Security Solutions

Technical Controls

- Multi-Factor Authentication (MFA)
- Firewalls
- Antivirus Software
- Database Encryption

Administrative Controls

- Security Awareness Training
- Access Control Policies
- Regular Audits

Physical Controls

- CCTV Monitoring
- Secure Server Rooms
- Backup Power Supply

Conclusion

MediCare Solutions faces numerous security threats from internal users, cybercriminals, and accidental incidents. The most serious threats include ransomware, phishing attacks, insider misuse, and SQL injection.

The NHS WannaCry attack demonstrated how cyberattacks can severely disrupt healthcare services. Therefore, implementing strong security controls, employee training, data encryption, and disaster recovery plans is essential to protect patient information and maintain continuous healthcare operations.