Ryan Christopher
MET CS695 – Assignment 1

1.

Security Policies	Security Requirements
Servers shall be physically isolated and only authorized personnel can access.	The hospital will have a server room containing the servers that will be locked at all times. The door will be opened via key card access.*
Backup of data shall be periodically done to deal with hardware failure, software problems, etc.	At the end of each day, a backup will occur that syncs the backup system to the information system.*
Every **patient** shall be uniquely and convincingly identified.	Each patient will have a unique patient ID generated by hashing their name and SSN.*
Only identified/authenticated subjects shall be granted the access to the information system.	Each employee should register an account on the information system using their own employee ID, and choose a unique user name. A password with a minimum length of 8, mixed with at least one number, one lower-case or upper-case letter, and one special character, is required.
The unsuccessful access attempts shall be well managed, e.g., the total number, the time between two consecutive unsuccessful access attempts, etc.	Servers will store logs of all unsuccessful access attempts to the information system to be reviewed by system administrators.*
Every **employee** shall be associated with a label that indicates its security level to access different data.	After authentication, employees should be assigned a role based on their identity. Access to different resources are controlled based on the role.
Onsite (inside hospital) computers shall restrict physical connection to other devices.	No USB drive, portable hard drive, or SD card can be connected to hospital computers. Hospital computers cannot be used to charge phones, tables, cameras, etc.
Login from offsite (outside hospital) devices shall enforce a stronger authentication mechanism.	Employees need to use both their password and RSA token (distributed by manager) to authenticate themselves when using their own devices at home to connect to the information system.
Data transmission between offsite (outside hospital) devices and servers shall be kept secure.	All remote access to the information systems needs to use HTTPS/TLS.
The system shall maintain complete, secure records of actions that affect security, e.g., adding a new user, changing the security level of a subject, etc.	All security changes will be processed as tickets and stored on the information system as records showing each change and who worked on it.*
The security controls that implement security must be protected against unauthorized change.	The security policy and its implementation can only be accessed by system administrators.

* indicates a security requirement that was added to a security policy not addressed after mapping

2.

Malware 1: Trojan Horse

If the employees use a software to connect to the hospital servers or work with patient's data, then a well-made Trojan Horse could act as the software and be downloaded by unsuspecting employees. Since Trojans can contain keyloggers, the false software could be used to collect the credentials of the employees who mistakenly download it. As a result, bad actors could gain access to the hospital's information system and upload the data elsewhere.

After I chose Trojan Horse, I decided to research if any have occurred in the healthcare industry, and to my surprise the first documented ransomware was distributed as a floppy disk at a World Health Organization AIDS conference in 1989. It was a Trojan Horse that would activate only after the targeted computer was powered on 90 times.

Consequences to this type of attack could be financially related as the hospital could need to pay to have the files removed, or require time as each device affected would need to be wiped. If the backups were not done recently, then there could be data loss as a consequence as well from the reimaged devices that had unsaved data.

Countermeasures to this attack would be well outlined applications and software that are from trusted sources as outlined in the hospitals SOP's for setting up devices as well as not giving all staff admin access to the hospital computers so that they would be unable to download or run software not approved for use in the hospital. In a case where the assets are already affected, then an effective countermeasure would be the collection and reimaging of all assets that were found using the malicious application.

Malware 2: Ransomware

If the servers were not physically isolated and easily accessed by non-authorized personnel, then a device containing ransomware could be connected to the information system. This could result in the staff being locked out of the hospital's system as well as the data being encrypted and threatened to be released. This action could be intentional or unintentional, as something as simple as connecting a phone or laptop to another computer in order to charge or transfer files would be enough for the ransomware to gain access.

Since ransomware frequently threatens to publicize the data that is on the device and the hospital's information system could contain HIPAA data, the hospital would likely be forced to comply with the demands in order to prevent heavy legal fees. In addition, the reputation of the hospital would also be diminished as patients would want their information to be secured, making the consequences both finance and reputation based.

An example of ransomware affected a company in the healthcare field is the Change Healthcare ransomware attack in February of 2024. According to Security Intelligence, the company made a payment of $22 million via Bitcoin to the BlackCat organization.

Countermeasures to this type of attack, aside from having hardware that is inaccessible to unauthorized personnel, would be hiring a third party to assist in decrypting the data affected by the attack. That being said, if the bad actors are threatening releasing sensitive data, then the hospital would likely need to have mitigation with the group threatening to release the data.

References:

The first known/documented Ransomware was a Trojan Horse-
https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf
https://www.knowbe4.com/aids-trojan

Change Healthcare Ransomware Incident-
https://securityintelligence.com/news/change-healthcare-22-million-ransomware-payment/