As an information security officer, the 3 principles that was violated inlcude:

Availalbiity, (CIA TRIAD/ Pakerian Hexad): violated because the ransom made the patients ifnormation in accessible wen the hospital wanted to access it. This disrupt the hospital of being able to work or staisfy its patients.

Integrity(CIA TRIAD/ Pakerain Hexad): Ransomware takes over the hospital data and even if the data is being retrieved, whats shows the data havent been tampered or modify.The hospital will not be able to get accuarte figures or information once it violates the integrity.

Possesion(Pakerian Hexad): violated because the hackers take control over the hospital data. This means the hospital lost control on their onw data.

Okay by introducing

1. Perimeter security(firewalls, IPS): This perimeter security is to ensure proper communication or protol rules that need to be assigend to devices that the hospiatl are using. This will also block any malcious attack the hackers will try to intrude in the system.

Data security: secure offline backup would allow recovery without paying a ransome. It controls will reduce unauthorized encryption of files.

Endpoint security: initiating this control in dveices will preveent a lot hackers from getting acces to the hsoiptal information.

Mnagers:

Attackers use sohpiscated phising emails, social engineering, zero-day exploits to bypass firewalls and antivirus.Security is not te only the technology to prevent hackers but the people and its processes matter as well.

Educationg staff on phishing and any suspicious attacks that might come on their way. Implementing strong password polcy or incident respond [lan.

Identification: Detect and confrim ransom attack

Conatianment: isolate affected system to prevent further spread.

Eradication: remove ransomeare and restore the system.

Recovery: restore the patient records from secure offline backup.

Lessone learnerd.

Identification: detect and confirm the ransomware.

Containment: isolated the affected system to prevent further spread.

Eradication: remove ransomware and restore the systekm

Recovery: restore system from secure backup offline.

Lessone learned: Strength defense, updating policies and educating staff.