Date: **2/09/2025**	**Entry: 1** Documenting a cybersecurity incident-US HealthCare Organization
Description	A phishing attack encrypted a U.S. healthcare clinic’s systems, demanding ransom. Employees lost access to medical records, forcing a shutdown. On Tuesday @ approximately 9AM, a small US Health Clinic organization that specializes in delivering primary care was attacked by an organization of unethical hackers. The attacked encrypted computers and resulted in employees not being able to access important files , such as medical record files, etc. Furthermore, this led to a total shutdown of the clinic. Employees also reported a ransom note from the hackers → large sum of money in exchange for the restoring access of the decrypted files. Hackers were abe to do this by phishing employees with an email that contained a malicious attachment that installed malware on employees computer onced accessed which led companies to shut off computer systems and temporarily shut down. The incident falls under **Detection & Analysis**, identifying phishing and malware, and **Containment, Eradication & Recovery**, involving system shutdown, malware removal, and recovery efforts to restore access to encrypted files.
Tools Used	
The 5 W’s	● **Who:**Organization of unethical hackers ● **What:** Installed malware on US healthcare computer systems ● **When:**On Tuesday at approximately 9 AM ● **Where:**Online via email (Phishing) ● **Why:**Ransom- Hackers want money in exchange for restoration of access.

Additional Notes	