Incident handler's journal

Date: May 16, 2025	**Entry:** 1
Description	This journal entry documents a ransomware attack that took place in a small U.S. health care clinic where attackers used phishing emails to infiltrate the network and encrypt sensitive files.
Tool(s) used	No specific cybersecurity tools were used during this documentation step. However, tools like Wireshark, Splunk or VirusTotal can be used for analysis.
The 5 W's	Capture the 5 W's of an incident. • **Who**: An organized group of unethical hackers known for targeting healthcare sectors. • **What**: Attackers used phishing emails to hack into the system, then deployed ransomware to encrypt sensitive files into the system and demanded a ransom payment. • **When**: Tuesday morning at 9am. • **Where**: Small healthcare clinic in the U.S. • **Why**: The attackers exploited human error by sending out phishing emails through which they got into the employees system and were able to encrypt important files. Their motive is likely to be financial gain as they have demanded a large amount of money in exchange for the decryption key.
Additional notes	This scenario highlights the critical importance of employee cybersecurity training, particularly in recognizing phishing emails. It also reinforces the need for robust email filtering, endpoint protection, as well as offline backups to recover from ransomware attacks without paying a ransom. Future steps could include incident containment, forensic investigation, and reporting the

	incident to higher authorities due to potential HIPAA violations.