Incident Handler’s Journal Entry

Name: Abubakari-Sadique Hamidu

Date: April 24, 2025

Assignment Type: Learning Simulation / Scenario Analysis

1. Scenario Overview

This entry is part of a cybersecurity training exercise. The scenario provided involves a simulated security incident at a small healthcare clinic in the United States. The goal is to practice proper documentation as an incident handler would during an actual response effort.

2. Incident Summary

On a simulated Tuesday at approximately 9:00 a.m., several employees at a small U.S.-based primary care clinic reported that they were unable to access files on their computers, including important medical records. This incident raised concern of a potential cybersecurity breach or system compromise.

3. Initial Observations

- Multiple users were locked out of critical systems.
- Attempts to open medical records failed, with errors or access denied messages.
- Systems displayed signs of unauthorized modification or encryption.
- The issue appeared to be widespread across departments.

4. Immediate Actions Taken

- Incident response procedures were initiated by IT staff.
- Affected machines were disconnected from the network to prevent further spread.
- Internal security team was alerted and began initial triage.
- Backups were reviewed to assess recovery options.

5. Potential Impact

- Disruption in access to patient health records and appointment systems.
- Inability to deliver primary care services during the incident window.
- Possible breach of Protected Health Information (PHI), leading to HIPAA concerns.
- Operational downtime and reputational risk to the healthcare provider.

6. Lessons Learned (Reflection)

This simulation highlights the importance of timely response, strong access control, and the value of maintaining regular system backups. Practicing incident documentation helps reinforce the core responsibilities of an incident handler in real-world scenarios.

This entry was created as part of a school assignment to practice cybersecurity incident documentation. It is based on a fictional scenario provided in a course module.