**Small Health Incident handler's journal**

| **Date:**  2024-01-31 | **Entry:**  JE-0001. | | |
| --- | --- | --- | --- |
| Description | Small Health Clinic Security Incident | | |
| Tool(s) used | NIST-CSF | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A phishing email that contained a malicious attachment. * **What** happened? Business operations were shut down as employees could not access medical records and files needed to perform their jobs. * **When** did the incident occur? The incident occurred on Tuesday 9:00am * **Where** did the incident happen? The incident happened on the company’s computer system and employee emails. * **Why** did the incident happen? There is not enough security awareness training for employees. | | |
| Additional notes | Include any additional thoughts, questions, or findings.  Most of the employees are not trained to identify phishing emails and how to handle them. | | |