MediHealth Clinic – Incident Response Plan (IRP)

Prepared by: **Taniesha Stewart** — 2025

This Incident Response Plan (IRP) establishes the framework and procedures for detecting, responding to, and recovering from cybersecurity incidents at MediHealth Clinic. 1. Purpose To ensure a timely, organized, and effective response to incidents that could impact confidentiality, integrity, or availability of systems and data. 2. Scope Applies to all employees, contractors, and third-party vendors who access MediHealth Clinic information systems. 3. Incident Response Phases - Preparation: Maintain policies, training, and tools. - Detection & Analysis: Monitor systems using SIEM and IDS tools. - Containment: Isolate affected systems to prevent spread. - Eradication: Remove malware or vulnerabilities. - Recovery: Restore operations using backups and validate system integrity. - Post-Incident Review: Conduct lessons learned and update response plans. 4. Roles & Responsibilities - Incident Response Team (IRT): Leads technical investigation and containment. - Compliance Officer: Ensures reporting obligations under HIPAA are met. - IT Security Manager: Oversees restoration and follow-up actions. 5. Communication Plan - Internal alerts through the ticketing system. - External notifications to affected patients and partners within 72 hours if PII/PHI is exposed. 6. Testing and Training - Annual tabletop exercises. - Quarterly phishing and response simulations.