HIPAA Gap Analysis – Acme HealthTech

# 1. Summary

This gap analysis evaluates Acme HealthTech’s compliance with HIPAA Security Rule safeguards. Several key deficiencies were identified, including lack of risk assessments, missing MFA controls, and absence of formal training programs. Addressing these gaps will significantly improve the organization’s compliance posture and resilience against data breaches.

# 2. Gap Analysis Table

|  |  |  |  |
| --- | --- | --- | --- |
| HIPAA Requirement | Current Status | Gap Identified | Recommendation |
| Risk Assessment | Not Performed | No documented risk assessment | Conduct and document a full risk assessment |
| Access Controls | Partially Implemented | No MFA on patient portal | Implement MFA and RBAC |
| Security Awareness Training | Not Implemented | No training program for staff | Launch annual training for all employees |
| Device and Media Controls | Not Implemented | No policy for device reuse/disposal | Develop and enforce media disposal policy |
| Audit Logs | Partially Implemented | Some systems lack logging | Enable centralized audit logging |
| Contingency Plan | Not Documented | No disaster recovery or backup plan | Create and test a contingency plan |