TESTING POLICY – HIPAA §164.312 TECHNICAL SAFEGUARDS

1. Purpose

This policy establishes technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) in accordance with 45 CFR §164.312 and §164.306.

2. Scope

This policy applies to all information systems, applications, users, workforce members, contractors, and third parties that access, store, transmit, or process ePHI.

3. Access Control (§164.312(a))

The organization implements technical policies and procedures to allow access to ePHI only to authorized users and systems.

- Unique user identification is assigned to each workforce member.
- Emergency access procedures are defined and tested annually.
- Automatic logoff is enforced after periods of inactivity.
- Encryption and decryption mechanisms are used to protect ePHI at rest and in transit.

4. Audit Controls (§164.312(b))

The organization implements hardware, software, and procedural mechanisms to record and examine system activity involving ePHI.

- Security logs are enabled on all systems containing ePHI.
- Audit logs capture user access, system changes, and security events.
- Logs are reviewed regularly by designated security personnel.

5. Integrity (§164.312(c))

The organization protects ePHI from improper alteration or destruction.

- Integrity controls are implemented to detect unauthorized changes.
- Mechanisms are in place to authenticate ePHI.
- Integrity monitoring alerts are reviewed and investigated.

6. Person or Entity Authentication (§164.312(d))

Procedures are implemented to verify that users and systems accessing ePHI are who they claim to be.

- Authentication mechanisms include passwords and multi-factor authentication.
- System-to-system authentication is enforced where applicable.

7. Transmission Security (§164.312(e))

Technical security measures are implemented to protect ePHI transmitted over electronic communications networks.

- Encryption is used for ePHI transmitted over public or unsecured networks.
- Integrity controls ensure transmitted ePHI is not improperly modified.

8. Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination, and may expose the organization to regulatory penalties.

9. Review and Maintenance

This policy is reviewed annually and updated as needed to ensure continued compliance with HIPAA Security Rule requirements.