HIPAA COMPLIANCE GUIDE

1. Protected Health Information (PHI)

Protected Health Information includes any individually identifiable health information held or transmitted by a covered entity. This includes demographic data, medical histories, test results, insurance information, and any other information used to identify a patient. PHI can exist in electronic, paper, or oral form. All forms must be protected equally under HIPAA regulations.

2. Privacy Rule Requirements

The Privacy Rule establishes national standards for the protection of PHI. Covered entities must implement appropriate administrative, technical, and physical safeguards. Patients have the right to access their medical records, request corrections, and obtain an accounting of disclosures. Healthcare providers must provide a Notice of Privacy Practices to all patients.

3. Security Rule Standards

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic PHI. This includes ensuring confidentiality, integrity, and availability of all ePHI. Risk assessments must be conducted regularly. Access controls, audit controls, and transmission security must be implemented.

4. Breach Notification Requirements

In the event of a breach of unsecured PHI, covered entities must notify affected individuals within 60 days. If the breach affects more than 500 individuals, the media must also be notified. The HHS Secretary must be notified of all breaches. A breach is defined as unauthorized acquisition, access, use, or disclosure of PHI.

5. Business Associate Agreements

Business associates are persons or entities that perform functions involving PHI on behalf of covered entities. A written Business Associate Agreement must be in place before sharing PHI. The agreement must specify permitted uses and disclosures, require appropriate safeguards, and mandate breach reporting.

6. Minimum Necessary Standard

Covered entities must make reasonable efforts to limit PHI access to the minimum necessary to accomplish the intended purpose. This applies to uses, disclosures, and requests for PHI. Policies must identify persons who need access and the categories of PHI needed. Role-based access controls should be implemented.