

HEALTHCARE PRIVACY POLICY

Section 1: Patient Data Privacy

All patient data must be protected in accordance with HIPAA regulations. Healthcare providers are required to implement appropriate safeguards to ensure the confidentiality, integrity, and availability of protected health information (PHI). Key requirements include encryption of all electronic health records, access controls limiting data access to authorized personnel only, audit trails for all data access and modifications, and secure disposal of physical and electronic records.

Section 2: Informed Consent

Healthcare providers must obtain informed consent before any medical procedure or treatment. The consent process must include clear explanation of the proposed treatment, discussion of risks and benefits, alternative treatment options, and the patient right to refuse treatment. Consent forms must be documented and retained in the patient medical record.

Section 3: Medical Record Retention

Medical records must be retained for a minimum of seven (7) years from the date of last patient encounter. For pediatric patients, records must be retained until the patient reaches age 21, or seven years from the last encounter, whichever is longer.

Section 4: Telemedicine Guidelines

Telemedicine consultations must adhere to the same privacy and consent requirements as in-person visits. Additional requirements include secure encrypted video platforms, patient identity verification, documentation of technical limitations, and emergency protocols for remote patients.

Section 5: Adverse Event Reporting

All adverse events must be reported within 24 hours of discovery. The reporting process includes immediate notification to supervising physician, documentation in incident reporting system, root cause analysis for serious events, and corrective action implementation.