HIPAA and Compliance Policies

These HIPAA and compliance policies are intended to support Canopy Therapy Solutions as a small healthcare practice that provides mobile, outpatient, facility-based, and telepractice services. They establish a practical framework for protecting protected health information, supporting regulatory compliance, and promoting consistent operations across clinical, administrative, and technology workflows.

Governance and Responsibility

Canopy Therapy Solutions will designate a responsible individual to oversee privacy, security, and compliance activities, maintain policies and procedures, coordinate staff training, and monitor corrective actions. Compliance oversight will include periodic review of operations, vendors, documentation standards, security safeguards, and complaint handling. When outside billing, technology, or administrative support is used, responsibilities will be defined in writing and monitored through routine oversight.

Privacy and Permitted Uses of Protected Health Information

The practice will use and disclose protected health information only as permitted by applicable law and only for legitimate treatment, payment, health care operations, or other authorized purposes. Staff and contractors will be expected to follow a minimum necessary standard when using, sharing, or accessing information, except where a broader disclosure is permitted or required for treatment or by law. Protected health information may exist in verbal, paper, electronic, photographic, or other recorded forms and will be safeguarded accordingly.

Notice of Privacy Practices and Patient Rights

The practice will maintain and make available a Notice of Privacy Practices that explains how patient information may be used and disclosed, what privacy rights patients have, and how concerns may be reported. Patients will be informed of their rights to access records, request amendments where applicable, request restrictions when permitted, request confidential communications, and receive an accounting of certain disclosures as required by law. Notice content and delivery practices will be reviewed and updated when material privacy practices change.

Workforce Access, Confidentiality, and Training

Access to protected health information and business systems will be role-based and limited to the functions necessary for each workforce member, contractor, or vendor. All workforce members will complete privacy, security, and confidentiality training at onboarding and at regular intervals thereafter, with additional training provided when policies, technology, or risk conditions change. The practice will require workforce members to follow password, device, communication, and documentation standards and to report suspected incidents promptly.

Administrative, Physical, and Technical Safeguards

The practice will implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Safeguards will include periodic risk analysis and risk management activities, secure configuration of devices and software, unique user credentials, strong passwords, multi-factor authentication where available, timely software updates, secure backup processes, audit logging when supported, and encryption or other protections for data at rest and in transit when feasible. Physical safeguards will include secure storage of paper records and devices, workstation privacy practices, visitor awareness, and controlled disposal of records and media.

Telepractice, Mobile Services, and Remote Work Safeguards

Because Canopy Therapy Solutions will deliver services in homes, facilities, and virtual environments, the practice will use secure platforms and workflows designed to reduce privacy and security risks outside a traditional office. Telepractice and remote access tools will be evaluated for appropriate privacy and security features before use, and vendors that create, receive, maintain, or transmit protected health information on behalf of the practice will be reviewed for business associate requirements. Staff will be expected to protect screens, maintain private surroundings when discussing patient information, use secure networks whenever possible, and avoid storing patient information on personal devices unless specifically authorized and protected.

Business Associates and Vendor Management

The practice will identify vendors and service providers that may access or handle protected health information, evaluate them for privacy and security risk, and maintain written agreements when required. Vendor oversight will include confirmation of service scope, data handling expectations, breach reporting responsibilities, and termination or data return procedures where appropriate. Examples may include electronic health record vendors, telepractice platform providers, cloud storage vendors, billing companies, IT service providers, and other third-party support services.

Records Management and Documentation

Patient records, billing records, compliance documentation, policies, training records, and related materials will be created, stored, retained, and disposed of according to legal, payer, and operational requirements. Documentation practices will emphasize accuracy, timeliness, completeness, and secure retention. The practice will maintain processes for record requests, release of information, corrections when appropriate, and secure destruction of records and media at the end of the applicable retention period.

Incident Response and Breach Notification

The practice will maintain an incident response process for suspected privacy, security, or cybersecurity events, including misdirected communications, unauthorized access, lost devices,

ransomware, or other potential compromises of protected health information. Workforce members will be expected to report suspected incidents immediately. Reported events will be documented, investigated, mitigated where possible, and assessed to determine whether notification obligations apply. If a reportable breach of unsecured protected health information is confirmed, notification will be provided in accordance with applicable legal requirements and required timeframes.

Sanctions, Complaints, and Corrective Action

Policy Review, Risk Monitoring, and Continuous Improvement

The practice will apply appropriate sanctions or corrective actions when workforce members fail to follow privacy, security, documentation, or compliance requirements. Patients and workforce members will have a process for reporting concerns or complaints without fear of retaliation. Reported concerns will be reviewed promptly, documented, and addressed through retraining, workflow changes, technical safeguards, disciplinary action, or other corrective measures as appropriate.