****MOBILE URGENT CARE**

HIPAA COMPLIANCE TRAINING CURRICULUM
(Privacy, Security, & Breach Prevention)**

I. Purpose of the Training

This curriculum ensures all Mobile Urgent Care (MUC) staff understand and comply with:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Breach Notification Rule
- 42 CFR Part 2 (when behavioral health or SUD info is involved)
- NC DHHS Medicaid & Medicare program integrity standards

The curriculum applies to all employees, contractors, volunteers, and business associates.

II. Target Audience

- Clinical staff (NPs, PAs, RNs, LPNs, EMTs, behavioral health professionals)
- Administrative and billing personnel
- Drivers and mobile unit techs
- Leadership and compliance teams
- Any individual handling PHI or ePHI

III. Training Format & Frequency

A. Required Training Schedule

- **Upon hire** (within first 24 hours of beginning work)
- **Annually** thereafter
- **Immediately** when regulations, policies, or systems change

B. Delivery Methods

- Instructor-led training (onsite or virtual)

- Self-paced online learning modules
- Case scenarios & simulated breach drills
- Quizzes and competency evaluations

IV. Curriculum Outline

MODULE 1 — Introduction to HIPAA

Learning Objectives

- Understand the purpose of HIPAA
- Recognize what constitutes Protected Health Information (PHI)
- Identify roles and responsibilities of workforce members

Topics Covered

1. Why HIPAA exists (fraud, privacy, national standards)
2. Terms: PHI, ePHI, covered entities, business associates
3. PHI in Mobile Urgent Care operations:
    - Paper charts
    - Electronic tablets/laptops
    - Voicemail & text messages
    - Telehealth
    - Transport & mobile units

MODULE 2 — The HIPAA Privacy Rule

Learning Objectives

- Protect PHI in all formats
- Apply minimum necessary standards
- Use & disclose PHI legally and safely

Topics Covered

1. Permitted uses and disclosures
2. Minimum necessary standard
3. Authorizations and consents
4. Patient rights under HIPAA:
    - Access
    - Amend
    - Restrict
    - Accounting of disclosures
    - Confidential communications
5. Treatment situations common to MUC:
    - Street-based care
    - Mobile vaccinations
    - Behavioral health screenings
    - Care coordination & referrals
6. Do's and Don'ts of PHI handling

Required Skill Practice

- Staff must practice de-identifying PHI
- Staff learn how to verify identity before sharing information

---

MODULE 3 — The HIPAA Security Rule

Learning Objectives

- Safeguard ePHI through administrative, physical, and technical protections

Topics Covered

1. Password security, multi-factor authentication
2. Laptop/tablet/ipad encryption

3. Mobile unit security (locked storage, secure WiFi)
4. Texting rules — permitted **only on HIPAA-approved platforms**
5. Secure documentation within EMR/EHR
6. Prohibited actions:
    - Using personal devices without authorization
    - Sharing logins
    - Unencrypted email or messaging
7. Physical safeguards:
    - Keeping mobile units locked
    - Ensuring printed documents are secured
    - Privacy screens in the field

Security Drills

- Lost/stolen device simulation
- Unauthorized visitor attempt

MODULE 4 — HIPAA & Behavioral Health / SUD (42 CFR Part 2)

Learning Objectives

- Understand enhanced privacy standards for SUD and mental health information

Topics Covered

1. Differences between HIPAA and **42 CFR Part 2**
2. When MUC must obtain specific written consent
3. Sharing information with:
    - Mobile Crisis
    - Hospitals
    - MAT providers
    - Law enforcement

4. Emergency exceptions

MODULE 5 — Breach Prevention & Breach Notification

Learning Objectives

- Know how to identify, report, and respond to suspected breaches

Topics Covered

1. What is a breach?
    - Wrong recipient
    - Lost or stolen device
    - Unauthorized access (internal/external)
2. MUC breach reporting timeline:
    - Report to Compliance Officer **within 24 hours**
    - Internal investigation by Compliance Team
    - Notifications following 45 CFR 164.400–414
3. How to preserve evidence
4. Documentation requirements
5. Role of the HIPAA Compliance Officer

Breach Simulation

- Each employee must complete a mock breach response scenario.

MODULE 6 — HIPAA, Medicaid Compliance & Fraud Prevention

Learning Objectives

- Prevent violations of HIPAA, Medicaid integrity rules, and CMS requirements

Topics Covered

1. HIPAA's relationship to:
    - NC Medicaid Program Integrity

    - CMS Conditions of Participation
    - OIG compliance requirements
2. Prohibited behaviors (examples relevant to MUC):
    - Discussing patient information inside the mobile unit with non-staff
    - Taking photos/videos with PHI in the background
    - Sharing PHI with partners or family
    - Using PHI for marketing without authorization
3. Documentation integrity:
    - Accurate clinical notes
    - No “copy & paste” errors
    - No falsification or backdating
4. Waste/Fraud/Abuse integration:
    - Billing only for services rendered
    - No upcoding
    - No falsified time sheets
    - No duplicate claims

MODULE 7 — Ethics & Professional Conduct

Learning Objectives

- Uphold high ethical standards when managing PHI

Topics Covered

1. Confidentiality as a core ethical principle
2. Professional boundaries in mobile environments
3. Non-discrimination & respect
4. Conflict of interest
5. Avoiding inappropriate conversations or gossip

6. Duty to report unethical behavior

Ethics Exercise

- Staff respond to real-world MUC scenarios involving confidentiality dilemmas.

MODULE 8 — Documentation, Storage, & Disposal of PHI

Learning Objectives

- Comply with state/federal rules for storing, retaining, and disposing of PHI

Topics Covered

1. Proper charting
2. File retention rules
3. Secure destruction (shredding, encrypted wipe)
4. Mobile unit-specific PHI disposal workflow
5. Chain-of-custody for PHI transport

MODULE 9 — Staff Competency Assessment

Includes

- 25-question HIPAA knowledge quiz
- Scenario-based evaluation
- Skills checklist (verifying identity, secure documentation, device safety)

Passing Requirement

- **80% minimum score**
- Remediation required for lower scores

MODULE 10 — Acknowledgement & Certification

Every staff member must sign:

- HIPAA Training Acknowledgement Form

- Confidentiality Agreement
- Mobile Urgent Care Privacy & Security Policy
- Code of Conduct and Ethics Statement

Each must be stored in the employee's personnel file.
