ChatRx & ChatMD Telehealth Location Regulation Policy

Requiring verifying patient identity and location

1. **Initial Identification**

   ◦ **Personal Information Verification:**

     ▪ Verify key personal information such as full name, date of birth, and address. Email, or phone number. Cross-check this information with the details provided during registration or previous medical records.

2. **Multi-Factor Authentication (MFA):**

   ◦ Implement MFA for logging into the telehealth platform. This typically involves:

     ▪ Something the patient knows (e.g., password or PIN).

     ▪ Something the patient has (e.g., a verification code sent to their phone or email).

3. **Patient Account Setup:**

   ◦ Require patients to create a secure account on your telehealth platform. This account should include:

     ▪ A unique username and strong password.

     ▪ Security questions or other verification methods.

4. **Electronic Consent Forms:**

   ◦ Have patients electronically sign consent forms that include their identification details. This helps verify their identity and provides legal documentation of their consent for telehealth services.

Verifying Patient Location

1. **Patient Address Confirmation:**

   ◦ **Initial Registration:**

     ▪ Collect and confirm the patient's address during the initial registration process.

   ◦ **Session Confirmation:**

     ▪ At the beginning of each paid telehealth session, ask the patient to confirm their current physical address.

2. **Geolocation Technology:**

   ◦ **IP Address Tracking:**

      ▪ Use IP address tracking to verify the patient's general location. This method helps confirm that the patient is within the geographic area where you are licensed to practice.

3. **Legal and Emergency Considerations:**

   ◦ **Emergency Situations:**

      ▪ Confirm the patient's location to ensure you can dispatch emergency services if necessary. Document the location in the patient's record.

   ◦ **State-Specific Compliance:**

      ▪ Ensure the patient's location complies with state regulations regarding where telehealth services can be provided. For instance, verify that the patient is physically located within Indiana or Michigan if those are the states where you are licensed.

Documentation and Record-Keeping

1. **Record Identity Verification:**

   ◦ Document the methods used to verify the patient's identity and location in the medical record. Include details such as the type of ID presented, and any additional verification steps taken.

2. **Telehealth Platform Security:**

   ◦ Ensure our telehealth platform is secure and complies with HIPAA regulations. This includes encrypting all data transmissions and maintaining secure access controls.

3. **Informed Consent:**

   ◦ Document the patient's informed consent for telehealth services, including the verification of their identity and location.

Technology and Platform Requirements

1. **Secure Telehealth Platform:**

   ◦ Use a telehealth platform that supports secure video conferencing, identity verification, and location tracking features. Ensure the platform is HIPAA-compliant.

2. **Regular Audits and Updates:**

   ° Conduct regular audits of your telehealth processes to ensure compliance with identity and location verification requirements. Update your procedures and technology as needed to maintain compliance.

Training and Policies

1. **Staff Training:**

   ° Train all staff involved in telehealth services on the procedures for verifying patient identity and location. Ensure they understand the importance of these steps for legal and clinical purposes.

2. **Written Policies:**

   ° Maintain written policies and procedures for verifying patient identity and location. Ensure these policies are accessible to all relevant staff members and are reviewed regularly.