Secure Electronic Communication & Patient Consent Policy

Sunflower Mountain Mental Health (SMMH)

Effective Date: *January 1, 2025*

Purpose

The purpose of this policy is to establish guidelines for secure electronic communication between Sunflower Mountain Mental Health (SMMH) staff, clinicians, and patients. This policy ensures compliance with **HIPAA, Medicare, Medicaid, and Colorado state regulations** while maintaining patient confidentiality and appropriate use of electronic communication methods.

Scope

This policy applies to all SMMH employees, contractors, and patients who engage in electronic communication, including email, text messaging, patient portals, and other digital communication platforms. It defines **acceptable communication methods, patient consent requirements, and staff responsibilities** to ensure secure and compliant electronic interactions.

Approved Communication Methods

SMMH authorizes the following electronic communication methods for staff, providers, and patients:

- **CharmHealth Patient Portal** – The **preferred** method for all patient communication related to care, scheduling, and billing.
- **Spruce Secure Messaging** – Used for **secure text messaging** between staff and patients.
- **Google Workspace – Healthcare Compliance Version** – Used by **clinicians and staff** for internal communication via **email, chat, and meetings**, as well as for patient forms submitted via **Google Forms and website-integrated forms**.
- **Telephone (Office Line or Spruce Calls)** – Used for **appointment scheduling and general inquiries**.
- **Secure Fax (Spruce e-Fax)** – Used for **medical records requests, prior authorizations, and referrals**.
- **Email & SMS Communication (With Patient Consent)** – Permitted for **brief scheduling and coordination** purposes only.

Prohibited Communication Methods

To ensure compliance with **HIPAA, Medicare, Medicaid, and Colorado healthcare regulations**, SMMH prohibits the use of the following communication methods for patient interactions:

- **Unencrypted Email and SMS for PHI** – Standard email and text messaging may not be used for sharing **protected health information (PHI)**, clinical discussions, or sensitive patient matters.
- **Social Media Messaging** – Platforms such as **Facebook, Instagram, Twitter (X), LinkedIn, and other social networks** may not be used for patient communication.
- **Third-Party Messaging Apps** – Personal or non-secure applications such as **WhatsApp, Signal, Telegram, Facebook Messenger, or other similar apps** are not permitted.
- **Personal Email or Messaging Accounts** – Clinicians and staff must use **SMMH-approved communication platforms** only. **Personal Gmail, Yahoo, or other private accounts** may not be used for any work-related communication involving PHI.
- **Voicemail Messages Containing PHI** – No PHI should be included in **voicemail messages** left for patients. Patients should only be instructed to return the call.
- **Unapproved Video Conferencing Platforms** – Any **non-HIPAA-compliant video platforms** (such as FaceTime, Skype, or Zoom outside of CharmHealth integration) may not be used for patient communication.

Relation to HIPAA Privacy Practices Policy

All electronic communication between SMMH staff, clinicians, and patients must comply with **HIPAA privacy and security regulations**. The **HIPAA Privacy Practices Policy** outlines:

- How patient PHI is collected, used, and shared.
- Patient rights to access, amend, and restrict their PHI.
- Protections against unauthorized disclosures of medical information.

Patient Consent for Electronic Communication

Before engaging in **email or text communication**, patients must provide explicit consent acknowledging the risks and limitations of these communication methods.

Consent Requirements

- Patients must **complete and sign** the **SMMH Email & Text Consent Form** before any electronic communication occurs.
- Consent must be **documented in the patient's electronic health record (EHR)**.
- Patients may **withdraw consent at any time** by notifying SMMH in writing or through the patient portal.

Patient Responsibilities & Acknowledgment

By providing consent, patients acknowledge the following:

- They have the option to communicate through **secure methods** (CharmHealth or Spruce) and are responsible for **requesting secure communication** if preferred.
- **Unencrypted email and text messages** are not fully secure and could be accessed by unintended parties.
- Electronic communication should only be used for **brief scheduling, coordination, or resource-sharing**—not for discussing **clinical matters** or **PHI**.
- **Urgent or emergency situations** should not be handled via email or text. Patients should call **911** or refer to the **Crisis & Emergency Response Policy**.
- Patients must **notify SMMH of any changes to their contact information** to ensure proper communication.

Permitted Uses of Email & Text Messaging

- **Scheduling and appointment reminders**
- **Billing and payment inquiries** (without PHI details)
- **General practice announcements**
- **Referrals and administrative questions**

Prohibited Uses of Email & Text Messaging

- **Clinical or medical discussions** (Patients should use the **CharmHealth Patient Portal** for clinical inquiries.)
- **Prescription requests** (Handled through **CharmHealth** or direct clinician consultation.)
- **Emergency or crisis communication** (Patients must call **911** or follow the **Crisis & Emergency Response Policy**.)

Withdrawing Consent

Patients may opt out of email and text communication at any time by:

- Sending a **written request** to SMMH via **secure message, email, or letter**.
- Requesting withdrawal **in person at an appointment**.

Upon receiving an opt-out request, SMMH will **update communication preferences within 5 business days**.

Staff & Clinician Responsibilities

All **SMMH clinicians and staff** are responsible for ensuring that electronic communication complies with **HIPAA, Medicare, Medicaid, and SMMH policies**.

General Communication Guidelines

- **Use only approved communication methods** for patient interactions (as outlined in this policy).
- **Verify patient identity** before discussing any sensitive health or financial information via phone, email, or text.
- **Redirect patients to secure platforms** (**CharmHealth or Spruce**) if they attempt to discuss PHI via unencrypted email or text.
- **Adhere to HIPAA's "Minimum Necessary Rule"**—only share the least amount of information required for patient care.
- **Ensure all patient consent for electronic communication** is documented in the **electronic health record (EHR)**.
- **Report any suspected security breaches** to the **SMMH Compliance Office immediately**.

Handling Non-Secure Communication Requests

- If a patient initiates communication via **unencrypted email or text**, staff must:
    - Inform the patient of the risks.
    - Redirect them to a **secure method**.
    - Refrain from discussing PHI via unapproved platforms.

Voicemail & Phone Communication

- **Do not leave PHI in voicemail messages**. Patients should only be instructed to return the call.
- **Verify the recipient's identity** before sharing any sensitive information over the phone.

Google Workspace & Internal Communication

- **Google Workspace (Healthcare Compliance Version)** is the only approved platform for **email, chat, and meetings** among staff and clinicians.
- PHI may only be shared internally through **Google Workspace** if **absolutely necessary and in compliance with the Minimum Necessary Rule**.
- Patient information collected through **Google Forms or website-integrated forms** must be **securely transferred to the EHR**.

Breach Prevention & Compliance Monitoring

- All electronic communication must align with **HIPAA, Medicare, Medicaid, and SMMH's HIPAA Compliance Policy**.
- **Security breaches must be reported per the SMMH Data Breach Notification Policy**.
- **Telehealth communication must comply with the SMMH Telehealth Compliance & Billing Policy**.

- **Regular audits of electronic communication** will be conducted to ensure compliance.
- **Violations of this policy may result in disciplinary action, up to and including termination**.

For additional information, refer to the following related policies:

- **HIPAA Compliance Policy**
- **Data Breach Notification Policy**
- **Telehealth Compliance & Billing Policy**
- **Crisis & Emergency Response Policy**
- **Discharge/Termination from Practice Policy**

Violations & Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination, in accordance with **SMMH policies, HIPAA regulations, and applicable federal and state laws**.

Staff & Clinician Violations

Violations by **staff or clinicians** may include but are not limited to:

- Using **non-approved communication methods** for patient interactions.
- Discussing **PHI over unencrypted email or text**.
- Failing to **redirect patients to secure platforms** when necessary.
- Leaving **PHI in voicemail messages** or sharing it improperly over the phone.
- **Not verifying patient identity** before discussing sensitive information.
- Failing to **report a suspected data breach** or unauthorized disclosure.

Patient Violations

While patients have the right to choose electronic communication methods, violations may include:

- **Repeatedly using non-secure communication** for PHI despite redirection to secure platforms.
- Sending **urgent or emergency messages via email or text** instead of using appropriate crisis resources.
- Failing to **update contact information**, resulting in miscommunication or security risks.

Enforcement & Corrective Action

- **Staff and Clinicians**

    - First-time violations may result in **a verbal warning and additional HIPAA training**.
    - Continued violations may lead to **formal disciplinary action**, including suspension or termination.
    - Intentional misuse of PHI or electronic communication methods may result in **immediate termination and potential legal consequences**.
- **Patients**
    - Patients who misuse electronic communication will be **reminded of the policy and redirected to secure platforms**.
    - Continued non-compliance may result in **communication restrictions** or, in severe cases, **termination of services**, as outlined in the **Discharge/Termination from Practice Policy**.

Reporting & Monitoring

- **All suspected policy violations** must be reported to the **SMMH Compliance Office immediately**.
- **Regular audits of electronic communication** will be conducted to ensure adherence to security standards.
- **Corrective action plans** will be implemented for any identified breaches or policy infractions.

Last Updated: *March 2025*

For further assistance, please contact SMMH at **(719) 679-5022** or visit www.sunflowermountainmentalhealth.com.