

FAMILY HEALTH & SPORTS MEDICINE

SMS Communication Policy

Terms & Conditions | Privacy Policy

Effective Date

June 1, 2026

Version

1.0

Compliance

HIPAA / TCPA

1. Introduction

This document establishes the SMS (Short Message Service) communication policy for our healthcare office (hereinafter referred to as the "Practice"). It governs all text message interactions between the Practice and its patients, caregivers, and authorized representatives.

Our Practice is committed to providing timely, convenient, and secure communication to support patient care. SMS messaging is used as a supplementary communication channel for appointment management, medication reminders, general health notifications, and administrative updates.

All SMS communications are conducted in strict compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Telephone Consumer Protection Act (TCPA), applicable state privacy laws, and industry guidelines set forth by the Cellular Telecommunications Industry Association (CTIA).

By opting into our SMS program, patients acknowledge and agree to the terms set forth in this document. Participation in the SMS program is entirely voluntary.

PART I: TERMS AND CONDITIONS

2. Consent and Opt-In

2.1 Obtaining Consent

The Practice obtains express written consent from patients or their authorized representatives prior to initiating any SMS communications. Consent is collected through one or more of the following methods:

- A signed consent form at the point of registration or check-in
- A digital opt-in form on the Practice's patient portal or website
- A keyword reply (e.g., "START", "YES", or "JOIN") to an initial enrollment message
- Verbal consent documented in the patient's electronic health record (EHR)

Consent is specific, informed, and unambiguous. Patients are clearly informed of the nature and frequency of messages they will receive before providing consent.

2.2 Opt-In Confirmation

Upon successful enrollment in the SMS program, patients will receive a confirmation message containing the following information:

- The identity of the Practice
- A brief description of the types of messages they will receive
- Estimated message frequency per month
- Instructions for opting out (STOP)
- A notice that message and data rates may apply
- A link to or reference to the full Privacy Policy

Example confirmation message:

FHSM: You have successfully enrolled in our SMS notification program. Msg frequency varies. Msg & data rates may apply. Reply STOP to unsubscribe, HELP for help. View our privacy policy at [URL].

2.3 Consent for Minors

For patients under the age of 18, consent must be obtained from a parent or legal guardian. All SMS communications involving minor patients will be directed to the consenting guardian's mobile number, unless otherwise authorized in writing.

3. Opt-Out and Unsubscribe

3.1 How to Opt Out

Patients may revoke their consent and opt out of receiving SMS messages at any time using any of the following methods:

- Reply "STOP", "CANCEL", "END", "QUIT", or "UNSUBSCRIBE" to any SMS message from the Practice
- Contact the Practice's front desk and request removal from the SMS program
- Log in to the patient portal and update communication preferences
- Submit a written request to the Practice's Privacy Officer

3.2 Opt-Out Confirmation

Upon receiving an opt-out request via SMS, the Practice will send a single, final confirmation message acknowledging the patient's request. No further promotional or informational SMS messages will be sent after the opt-out is processed, except as required by law or for critical safety notifications.

Example opt-out confirmation:

[Practice Name]: You have been unsubscribed from our SMS alerts. You will receive no further messages. To re-enroll, reply START or contact our office.

3.3 Re-Enrollment

Patients who have opted out may re-enroll in the SMS program at any time by replying "START" to a Practice number, contacting the office, or completing a new consent form. Re-enrollment constitutes renewed consent under these Terms and Conditions.

4. Types of SMS Communications

FHSM uses SMS messaging exclusively for the following categories of communication. Messages containing sensitive Protected Health Information (PHI) will only be sent with explicit patient authorization and appropriate security safeguards.

Category	Examples	PHI Included?
Appointment Reminders	Upcoming visit alerts, scheduling confirmations	Limited (date/time only)
Patient Initiated SMS	Your finger looks like it may be fractured and require immediate attention from an ER. Please go to your ER of choice for emergency treatment.	Limited
Medication: Prescription Prior Authorization Outcomes	Your Prescription for Ozempic has been approved. Please check with your pharmacy for pick-up time.	Limited
Emergency Notifications	Office closures, urgent safety alerts	No

5. Message Frequency and Costs

5.1 Message Frequency

The Practice will send no more than a reasonable number of SMS messages per patient per month, commensurate with the patient's care needs and preferences. Typical frequency is between 0 and 12 messages per month. Patients enrolled in specific care management programs may receive additional messages as clinically appropriate.

5.2 Carrier Fees

Message and data rates may apply depending on the patient's wireless carrier and mobile plan. FHSM is not responsible for any fees charged by a patient's mobile carrier for sending or receiving SMS messages. Patients are encouraged to review their mobile plan for applicable rates.

5.3 Help Keyword

Patients may reply "HELP" at any time to receive assistance. The following response will be sent:

FHSM SMS Help: For assistance, call 401-943-6910 or visit <https://fhsmri.com>. Reply STOP to unsubscribe. Msg & data rates may apply.

6. Prohibited Uses

FHSM expressly prohibits the following uses of the SMS program:

- Transmitting detailed clinical diagnoses, treatment plans, or full test results via SMS without explicit written patient authorization and appropriate security measures
- Sending unsolicited marketing or promotional messages unrelated to patient care
- Contacting patients regarding third-party products or services
- Transmitting any information that violates HIPAA privacy standards
- Sending messages to phone numbers provided without proper consent
- Using automated messaging in a manner that violates the TCPA

7. Patient Responsibilities

By participating in the SMS program, patients agree to:

- Provide accurate and current mobile phone number information
- Notify the Practice promptly of any changes to their mobile number
- Ensure that the mobile device is accessible only to the patient or authorized individuals
- Not share login credentials or one-time passcodes received via SMS
- Promptly notify the Practice if they suspect unauthorized access to their SMS communications
- Understand that SMS is not an appropriate channel for medical emergencies

In the event of a medical emergency, patients must call 911 or proceed to the nearest emergency room immediately. SMS messages may not be monitored in real time and are not suitable for urgent medical inquiries.

8. Limitations and Disclaimers

The Practice makes no warranty, express or implied, regarding the availability, reliability, or timeliness of SMS delivery. Delivery of SMS messages is subject to network availability and carrier limitations beyond the Practice's control.

The Practice reserves the right to modify, suspend, or terminate the SMS program at any time with reasonable notice to enrolled patients. Continued participation following any modification constitutes acceptance of the revised terms.

SMS communications are not a substitute for in-person consultations, telephone calls, or secure patient portal messaging when such communications are more clinically appropriate.

PART II: SMS PRIVACY POLICY

9. Information We Collect

9.1 Data Collected via SMS Enrollment

When a patient enrolls in the SMS program, the Practice collects and stores the following information:

- Patient's full name and date of birth (for identity verification)
- Mobile phone number
- Date and method of consent
- Preferred message types and communication preferences
- Opt-in and opt-out history

9.2 Data Generated During SMS Interactions

The following data may be generated and retained as part of the SMS communication record:

- Message delivery status (sent, delivered, failed)
- Timestamps of messages sent and received
- Inbound keyword replies (e.g., STOP, HELP, CONFIRM)
- Patient-initiated free-text responses, where applicable

9.3 What We Do Not Collect

The Practice does not use SMS communications to collect sensitive financial information, social security numbers, or detailed clinical data. Any clinical data shared via SMS (where expressly authorized) is governed by the Practice's Notice of Privacy Practices under HIPAA.

10. How We Use SMS Data

Information collected through the SMS program is used solely for the following purposes:

- Delivering appointment reminders and scheduling-related communications
- Sending administrative and care coordination notifications
- Managing opt-in and opt-out preferences
- Improving the quality and relevance of our patient communications
- Compliance with legal, regulatory, and accreditation requirements
- Investigating and resolving complaints or disputes related to SMS communications

The Practice does not use SMS data for targeted advertising, population health marketing without consent, or any commercial purpose unrelated to patient care.

11. Sharing and Disclosure of SMS Data

11.1 Business Associates

The Practice may engage third-party SMS platform providers and technology vendors ("Business Associates") to facilitate the delivery of SMS messages. All Business Associates are required to execute a HIPAA-compliant Business Associate Agreement (BAA) and are contractually obligated to safeguard patient information.

11.2 Legal Requirements

The Practice may disclose SMS-related information when required by law, including in response to lawful subpoenas, court orders, regulatory investigations, or as required under HIPAA's required disclosures provisions.

11.3 No Sale of Information

The Practice does not sell, rent, trade, or otherwise transfer patient mobile phone numbers or SMS interaction data to third parties for commercial purposes. This prohibition applies without exception.

11.4 Emergency Disclosures

In rare circumstances involving imminent risk to the safety of the patient or the public, the Practice may disclose relevant information consistent with HIPAA's emergency exception provisions (45 CFR §164.512(j)).

12. Data Security

12.1 Technical Safeguards

The Practice implements administrative, physical, and technical safeguards to protect SMS data, including:

- Encryption of data in transit and at rest where technically feasible
- Role-based access controls limiting SMS data access to authorized personnel
- Regular security risk assessments in accordance with HIPAA Security Rule requirements
- Secure, audited platforms for SMS delivery that meet healthcare industry standards
- Multi-factor authentication for staff accessing the SMS management platform

12.2 Limitations of SMS Security

Patients are advised that standard SMS messages (non-encrypted text messages) transmitted over cellular networks are inherently less secure than communications sent via the Practice's encrypted patient portal. Although the Practice takes reasonable precautions to protect message content, no method of electronic communication is completely secure. Patients are encouraged to use the patient portal for any communications involving detailed health information.

12.3 Breach Notification

In the event of a security breach affecting SMS data that constitutes a breach of unsecured PHI under HIPAA, the Practice will notify affected patients and relevant regulatory authorities in accordance with the HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D) and applicable state law.

13. Data Retention

SMS records, including consent logs, message delivery records, and opt-out history, are retained in accordance with applicable federal and state medical records retention requirements. Generally, SMS consent and communication records are retained for a minimum of six (6) years from the date of creation, consistent with HIPAA requirements, and 7 years from the date of creation, consistent with State of Rhode Island regulations.

Upon receipt of a written request for deletion of non-clinical SMS records, the Practice will evaluate and respond to such requests in compliance with applicable law. Note that certain records may be required to be retained regardless of patient preference.

14. Patient Rights

14.1 Right to Access

Patients have the right to request access to records of their SMS communications with the Practice. Requests should be submitted in writing to the Practice's Privacy Officer.

14.2 Right to Correct

Patients may request corrections to inaccurate contact information or consent records maintained by the Practice.

14.3 Right to Restrict

Patients may request that the Practice restrict the use of SMS for certain categories of communication while maintaining enrollment for others (e.g., receiving only appointment reminders and opting out of billing notifications).

14.4 Right to Complain

Patients who believe their privacy rights have been violated may file a complaint with the Practice's Privacy Officer, or directly with the U.S. Department of Health and Human Services Office for Civil Rights (OCR) at www.hhs.gov/ocr without fear of retaliation.

15. Compliance Framework

The Practice's SMS program is designed to comply with all applicable laws and regulations, including:

Regulation / Standard	Applicability
HIPAA Privacy Rule	Governs use and disclosure of Protected Health Information (PHI) in all communications
HIPAA Security Rule	Requires administrative, physical, and technical safeguards for electronic PHI

HIPAA Breach Notification Rule	Mandates patient and regulatory notification in the event of a PHI breach
TCPA (47 U.S.C. § 227)	Regulates autodialed and pre-recorded calls/texts; requires prior express written consent
CTIA Guidelines	Industry best practices for commercial and healthcare SMS messaging programs
State Privacy Laws	Additional protections may apply depending on patient and Practice jurisdiction

16. Updates to This Policy

The Practice reserves the right to update this SMS Policy at any time. Material changes will be communicated to enrolled patients via SMS with a link to the updated policy, through the patient portal, or by other appropriate means. The effective date at the top of this document will reflect the most recent revision.

Continued participation in the SMS program following notice of policy updates constitutes the patient's acceptance of the revised terms.

17. Contact Information

For questions, concerns, or requests related to the SMS program or this Privacy Policy, patients may contact:

Privacy Officer	Lori J. Mosby
Mailing Address	65 Sockanosset Cross Road, Suite 301, Cranston, RI 02920
Phone	(401) 943-6910
Email	Ljmosby@fhsmri.com
Patient Portal	EPIC (Care New England Platform)
Office Telephone Hours	Monday – Thursday, 8:30 AM – 4:30 PM; Friday, 8:00 AM – 3:00 PM (local time)

PATIENT ACKNOWLEDGMENT

By enrolling in the SMS program (via keyword reply, signed consent form, or patient portal opt-in), the patient confirms that they have read, understood, and agreed to the SMS Terms and Conditions and Privacy Policy set forth in this document.

Patients are encouraged to retain a copy of this document for their records. A copy is also available upon request from the Practice's front desk or Privacy Officer.

Patient Signature

Date

Printed Name

Patient Date of Birth

Mobile Phone Number to Enroll

*This document constitutes the complete SMS policy of FHSM as of the effective date noted on the cover page.
For internal use and patient distribution.*