CMS Messaging Policy: SMS, MMS, Conversations, Third-Party Messaging Platforms

Last Updated: December 5, 2024

This Messaging Policy applies to SMS, MMS, Conversations, and Third-Party Messaging Platform channels. We all expect that the messages we *want* to receive will reach us, unhindered by filtering or other blockers. An important step CMS can take to make that expectation reality is to prevent and eliminate *unwanted* messages. Towards that end, we strive to ensure that messages are sent with the consent of the message recipient, and that those messages comply with applicable laws, communications industry guidelines or standards, and measures of fairness and decency.

CMS SMS Messaging

CMS treats all messaging transmitted are subject to this Messaging Policy, which covers rules and /or prohibitions regarding:

- Consent (“opt-in”);
- Revocation of Consent (“opt-out”);
- Sender Identification;
- Messaging Usage;
- Filtering Evasion; and
- Enforcement.

Consent / Opt-in

What Is Proper Consent?

Consent won’t be bought, sold, or exchanged.

Consent Requirements

- Prior to sending the first message, CMS will obtain agreement from the message recipient to communicate with them - this is referred to as "consent", CMS will make clear to the individual they agree to receive messages of the type you're going to send. CMS will keep a record of the consent, such as a copy of the document or form that the message recipient signed, or a timestamp of when the customer completed a sign-up flow.
- If CMS does not send an initial message to that individual within a reasonable period after receiving consent (or as set forth by local regulations or best practices), then CMS will reconfirm consent in the first message you send to that recipient.
- The consent applies only to the specific use or campaign that the recipient has consented to. CMS will not treat it as blanket consent.

- Proof of opt-in consent will be retained for 365 days or as set forth by local regulation or best practices after the end user opts out of receiving messages.

Alternative Consent Requirements

While **consent is always required** and the consent requirements noted above are generally the safest path, there are two scenarios where consent can be received differently.

Contact initiated by an individual

If an individual sends a message to CMS, CMS is free to respond in an exchange with that individual. For example, if an individual texts CMS's phone number asking for your hours of operation, CMS may respond directly to that individual, relaying your open hours. In such a case, the individual's inbound message to you constitutes both consent and proof of consent. The consent is limited only to that particular conversation. Messages that are outside that conversation will not be sent without confirming consent.

Informational content to an individual based on a prior relationship

CMS may send a message to an individual where we have a prior relationship, provided that individual provided their phone number to CMS, and has taken some action to trigger the potential communication, and has not expressed a preference to *not* receive messages from CMS. This includes appointment reminders, order/shipping/reservation confirmations, and drivers coordinating locations.

The message will not attempt to promote a product, convince someone to buy something, or advocate for a social cause.

Periodic Messages and Ongoing Consent

If circumstances arise where CMS intends to send messages to a recipient on an ongoing basis, CMS will confirm the recipient's consent by offering them a clear reminder of how to unsubscribe from those messages using standard opt-out language (defined below). CMS will also respect the message recipient's preferences in terms of frequency of contact. CMS will proactively ask individuals to reconfirm their consent as set forth by local regulations and best practices.

Identifying Yourself as the Sender

Every message CMS sends will clearly identify CMS as the sender, except in follow-up messages of an ongoing conversation.

Opt-out

The initial message that CMS will send to an individual will include the following language: "Reply STOP to unsubscribe."

Individuals will have the ability to revoke consent at any time by replying with a standard opt-out keyword. When an individual opts out, CMS may deliver one final message to confirm that the opt-out has been processed, but any subsequent messages are not allowed. An individual must once again provide consent before CMS can send any additional messages.

Usage Limitations

Content We Do Not Allow

CMS prohibits sending any content that is illegal, harmful, unwanted, inappropriate, objectionable, confirmed to be criminal misinformation, or otherwise poses a threat to the public, even if the content is permissible by law. Other prohibited uses include:

- Anything that is illegal in the jurisdiction where the message recipient lives. Examples include, but are not limited to:
    - *Cannabis.* Messages related to cannabis are not allowed in the United States as federal laws prohibit its sale, even though some states have legalized it. Similarly, messages related to CBD are not permissible in the United States, as certain states prohibit its sale. Twilio defines a cannabis message as any message which relates to the marketing or sale of a cannabis product, regardless of whether or not those messages explicitly contain cannabis terms, images, or links to cannabis websites.
    - *Prescription Medication.* Offers for prescription medication that cannot legally be sold over-the-counter are prohibited in the United States.
- Hate speech, harassment, exploitative, abusive, or any communications that originate from a hate group.
- Fraudulent messages.
- Malicious content, such as malware or viruses.
- Any content that is designed to intentionally evade filters.
- Any content related to alcohol, firearms, gambling, tobacco, or other adult content.

Messaging Policy Violation Detection and Prevention Evasion

CMS will not use the SMS platform to evade unwanted messaging detection and prevention mechanisms.

Examples of prohibited practices include:

- Content designed to evade detection. As noted above, we do not allow content which has been specifically designed to evade detection by unwanted messaging detection and prevention mechanisms. This includes intentionally misspelled words or non-standard opt-out phrases which have been specifically created with the intent to evade these mechanisms.

- Snowshoeing. We do not permit snowshoeing, which is defined as spreading similar or identical messages across many phone numbers with the intent or effect of evading unwanted messaging detection and prevention mechanisms.
- Simulated social engineering attacks. You are prohibited from transmitting messages that are used for security testing, including simulated phishing and other activities that may resemble social engineering or similar attacks.
- Other practices identified and prohibited by this policy and Twilio's Acceptable Use Policy.

How We Handle Violations

When we identify a violation of these principles, where possible, we will work with providers in good faith to get them back into compliance with this policy. Disciplinary actions may be taken against CMS employees per the Employee Handbook.