

Texting for public benefits

An informal collection of resources and guidance for governmental parties looking to send text messages for public benefits.

September 2024

# Disclaimer

The following represents a collection of resources, guides, recommendations, and practices for governments interested in texting for the purposes of administering public benefits. **This information is NOT a source of authoritative, legal, or regulatory guidance.** This guide has not been officially endorsed by any federal benefit administering agency. It is advisory only, and should be adapted appropriately for each scenario. Ultimately, it is the responsibility of the implementing party to ensure that any project is compliant with federal, state, and local statute and regulations. Refer to the federal administering agency for up-to-date official guidance.

# About this guide

This guide is intended to assist a governmental benefits agency with **no or little texting capability** with setting up a new texting program. It covers the **basics;** who can send texts, who can’t, and how to put the first few pieces in place.

This guide makes allusions to more advanced scenarios, **but does not explore them in depth**. As such, for states with existing texting programs, this guide may provide new ideas but will not focus on them.

This guide is intended to be a living document! If you have feedback, comments, or questions, please reach out to [phe-renewals@usds.gov](mailto:phe-renewals@usds.gov).

Table of Contents

[Disclaimer 2](#_Toc177547557)

[About this guide 2](#_Toc177547558)

[Authorization and legal 4](#_Toc177547559)

[Setting up a program 7](#_Toc177547560)

[Content 12](#_Toc177547561)

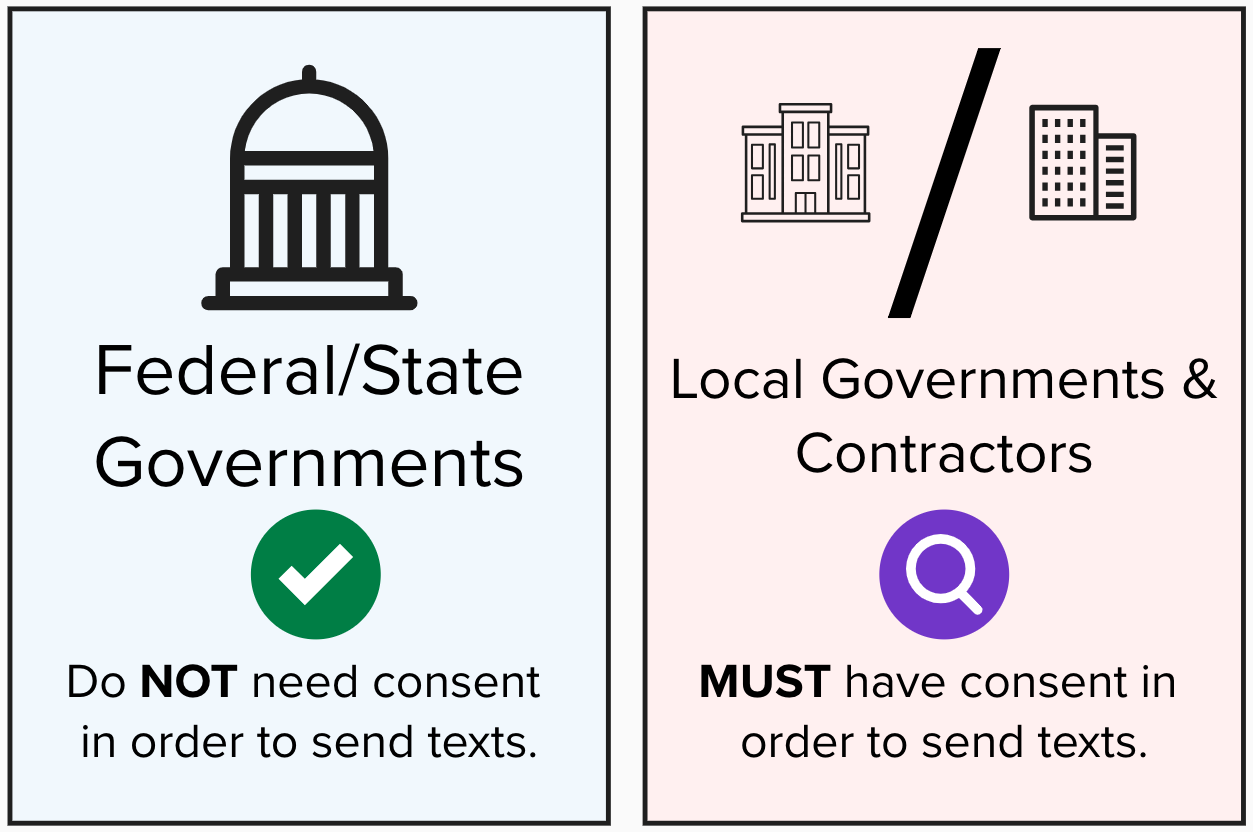
[Appendix A: WhatsApp 14](#_Toc177547562)

# Authorization and legal

## Who is allowed to send texts, and when?

The ability to *automatically* text is restricted by the Telephone Consumer Protection Act (TCPA). The TCPA mostly deals with “auto-dialers” making phone calls, but in 2003 the Federal Communications Commission (FCC) put out a ruling[[1]](#footnote-1) clarifying that the TCPA also applies to texting. In short, the TCPA says that an entity **cannot** automatically send texts unless they receive the **consent** of the person being texted.

**However:** in January 2023, the Federal Communications Commission (FCC) put out a ruling[[2]](#footnote-2) that said state and federal governments using texting for benefit programs were **not bound by the TCPA**. That is: state governments **can automatically text their beneficiaries without consent**, but local governments and non-governmental parties (like contractors) **must get consent**.



### Local governments and contractors

Local governments and contractors **must get consent** before texting. For what this looks like, see “What does consent look like?” below.

Note that most state governments use a contractor’s **platform** to actually send texts! In the FCC training and ruling, it clarifies that if the state or federal governments are the **“maker” of the text** (meaning they *physically* initiated it), then they are the “caller” and consent is not required.

Some states administer their benefit programs at the county level. These counties, if making texts, likely need consent.

#### What does consent look like?

Consent means someone has consented, either orally or written, to be texted at a given number about a benefit program.

The 2023 ruling stated that providing a phone number on an application for benefits **is written consent for the purposes of eligibility**. This can also look like pre-checked check box, with plain language for opt in (for example, “it’s okay to text me”)[[3]](#footnote-3).

If a person’s number has changed, their **consent is no longer valid**. In order to avoid texting a number that’s been reassigned recently, the FCC provides the Reassigned Numbers Database (RND)[[4]](#footnote-4) so that the number can be checked beforehand. It can be useful to store timestamps along with people’s phone numbers to determine how old they are!

### Tribal nations

The FCC didn’t clarify this in their ruling or training, but the *assumption* they voiced was that tribal nations, as sovereign entities, would be considered “federal governments” and **not subject to the consent requirements**.

## Texting for specific benefit programs

### Non-healthcare benefit programs

Even though the ruling was *addressed* to Health and Human Services (HHS), **the decision applies to non-healthcare programs** as well for the following reasons:

* The ruling itself specifies that it applies to “federal and state governments making calls in the conduct of official business” in paragraph 4 (this also applies to texting).
* The FCC put out a training[[5]](#footnote-5) that clarifies this ruling applies to all official business.
* CBPP also recommends[[6]](#footnote-6) the ruling be interpreted for all benefit programs.

### Texting about benefits the client hasn’t applied for

Giving consent to be texted about one benefit **does not** mean a person has consented to be texted about other benefits. For example, if someone has applied for SNAP and provided their phone number, they’ve consented to be texted about SNAP eligibility **only**; they haven’t consented to Medicaid.

This can be alleviated by **including language on the application** that allows for “sharing” consent (i.e. “I consent to be contacted at this number for additional benefits…”)

## WhatsApp/Telegram/Signal/etc.

WhatsApp, Telegram, and Signal are all examples of **Internet-based** messaging systems, meaning they don’t use SMS for sending a message to a user. The FCC considers these systems to be in a “regulatory-free arena”[[7]](#footnote-7), meaning the TCPA does not apply to them in general. **However,** it’s probably a good idea to treat these as if they are (or will be) regulated!

For WhatsApp, see Appendix A.

## Opting out

A recent FCC ruling clarified that, **for states that are not bound by the TCPA consent rules, an opt-out is not required[[8]](#footnote-8).** In general, though, it’s a best practice to have an opt-out system. See “Opt-out” in the following sections for more information.

# Setting up a program

This document covers a **very simple** (and recommended) texting program, in which texts are sent one-way to recipients.

There are three main components to setting up a texting program:

1. One or more use cases
2. An operational plan
3. An evaluation plan

## Use cases

When starting a texting program, align on **a small number of use cases** (ideally one to start). These use cases should meet the following criteria:

**Relevant**: The use case should address a clearly understood problem the state is having. Ideally, this problem is measurable with data.

**Clearly defined**: The recipients, content, and timing of the messages should be understood.

**Simple**: Texting can get complicated fast, which increases risk. Push the state to define the use case in the simplest way possible.

All use cases should have the following components **clearly defined**: recipients, content, and timing.

### Recipients

Recipients are the **people receiving the messages**; these are generally the participants (or applicants, if they are not participating already) in the benefit program. The recipients are defined via a category.

**Examples:**

* Applicants who have an interview scheduled for today’s date.
* Beneficiaries who have a recertification due in 14 days and have not completed it.
* Households who have a request for verification due and have not completed it.

It’s important to think about languages when defining the recipients. An initial pilot may limit the recipients to English speakers for convenience, **but should include a plan to expand to all language groups**.

### Content

The content of the message doesn’t need to be exact in the use case; at this point, general is fine. Content will be refined at a later step. However, it’s important to remember that **shorter is almost always better**.

Some tools will allow for customized messages for each sender (for example “Your interview is at 10:00 today” versus “Your interview is today”). While customized messages are generally more useful, they’re also more complicated to implement.

**Examples:**

* A reminder that an interview is scheduled, with instructions on what to expect.
* A reminder that a recertification is due, with instructions on how to get help.
* A reminder that a verification is due, with instructions on how to submit it.

### Timing

There’s room to be flexible with timing, but **simpler is almost always better**. In the simplest case, texts are sent all at once at a set time each day (ex: 10:00 AM, Monday-Friday). Sending each individual text at a specific time increases complexity; defining that time dynamically increases complexity further.

Keep in mind **weekends**. For example, if you’re sending reminder texts 24 hours before an interview, will someone need to be in the office on Sunday to send them? Or will they send it the Friday before? Will the text say “your interview is tomorrow”? Or “your interview is Monday”?

**Examples:**

* Texts are sent Mondays through Fridays at 10:00 AM in the local timezone.
* Texts are sent one hour prior to the scheduled interview time.
* Texts are sent when interview traffic is low.

### Operational plan

An operational plan for the initial texting program should detail the following pieces:

* The data (or “report”) that lists the numbers that will be texted and any metadata
* The tool used to send the texts
* The people involved (if any)
* (Recommended) An opt-out mechanism

#### The data

Before sending texts, the state needs to pull **the data** of the people to text. Most times, this looks like **a report**, often in CSV or Excel format. In the most minimal case, the report only consists of the phone numbers to text; in that case, everyone is receiving the same content! In the case of customized messages, this report may need to be more complicated.

The report will likely come from the eligibility system, and can be manually pulled or automatically pulled. Remember that you can pull **multiple reports**! For example, you might pull one report for English-speaking recipients, another for Spanish, etc.

If the texting tool supports API hookups, this can be a more complex (but automated) process, in which the data is automatically pulled **as JSON** (or another data format) and send automatically to the tool.

#### The tool

The texting tool **automatically sends the texts** when it receives the data (either by a person uploading a report, an API call, or some other method). If you already have access to a texting tool, using it will likely be easier than finding another one. However, when evaluating tools, some factors to keep in mind are:

* **Manual versus automatic**: Does the tool allow for someone to upload a file through a website and send the texts (manual)? Does it allow for an API hookup to send texts from a system (automatic)? Both?
* **Cost**: How much does a text cost? How many texts per day will you be sending?
* **Other message types**: Does the tool do texts only? Does it do email? Internet messages (like WhatsApp)? Which message types will you need?
* **Customer support**: Does the tool provide training and assistance to get started?

#### The people

In the ideal scenario, the entire texting program can be **automated**. However, this is often beyond the capacity of the state to setup quickly. In the meantime, a **manual process is totally acceptable**!

The activities needed to run a *simple manual texting program* are usually very low-effort:

* Pulling the report
* Uploading the report to the tool

The frequency, complexity, and volume of the texts can make these tasks easier or harder.

#### Opt-out mechanism

**Local governments and contractors are required to have an opt-out mechanism. State and federal governments are not,** but it’s best practice to have one. Fortunately, mobile networks *already provide* an opt-out mechanism; texting “STOP” to a phone number will block all future texts from that number. Many texting tools also honor these messages.

If a sender is building their own opt-out mechanism, best practices are:

1. Look for “STOP”, “QUIT”, “END”, “REVOKE”, “OPT OUT”, “CANCEL”, or “UNSUBSCRIBE” messages.
2. Allow people to opt-out **over the phone**, or by walking into an office.
3. Once someone has opted out, remove their number from texts within **24 hours**.
4. Within five minutes of the opt-out, send **one final message** confirming that the number is opted out, and providing instructions on how to opt in again.

If a sender is covered by the TCPA (i.e. they are a county or contractor), then this opt-out mechanism **is required**.

## Evaluation Plan[[9]](#footnote-9)

The evaluation plan is the means by which the state determines **if their text messages are achieving the desired result.** Prior to sending text messages, the state should determine one or more **output metrics** they desire to change, a reliable method of obtaining those metrics, and a baseline metric.

### Before/after

In the simplest case, the output metrics for the group that **received texts** is compared to the **baseline**. This may be sufficient for some programs, but is vulnerable to external bias.

### Experiment/control

A more rigorous setup would be to randomly divide the potential recipients into an **experiment and control** group. The texts are sent to the experiment group only. Afterwards, the output metrics for the experiment group are compared to the control group.

This setup is more complex, but provides **much more certainty** in the results of evaluation.

# Content[[10]](#footnote-10)

Content development is often the most time-consuming step of starting a texting program. Everyone will have thoughts on what the messages should say, but it’s important to develop them in a user-centered way.

## Policy and legal

Policy and/or legal should be involved throughout the content generation process. Their input will ensure that all messages are compliant with the policies of the state.

### Personal Health Information (PHI)

Often times there can be concern that sending text messages constitutes a transmission of PHI over an unencrypted channel. While it’s true that SMS is unencrypted, **the content of the text messages is very unlikely to be considered PHI**. Many states send text messages about public benefits without penalty. Prior to drafting, develop a clear definition of what constitutes PHI, and use these guidelines to develop a first draft.

## Drafting

Working in a small group, come up with **the first draft** of the message content. In general drafts should be all of the following:

**Identifiable** – They should specify that they are from the state benefit agency. This can be very short, such as starting the message with “Alaska SNAP:”

**Actionable** – The messages should clearly indicate what is needed from the client.

**Plain language** – The first draft should be written such that it is understandable by recipients with a range of reading abilities.

It can be useful to start with other state’s texting efforts; some examples are available from [Code for America’s LA’MESSAGE pilot](https://integrated-benefits.s3.us-east-2.amazonaws.com/Text+Message+Scripts.pdf) in Louisiana.

## Testing and iteration

After drafting, the content should be tested with **people close to the recipients** receiving the message. These people may fall into one of the following categories (but can be outside of them as well):

**Eligibility Workers** – Workers who regularly interact with recipients

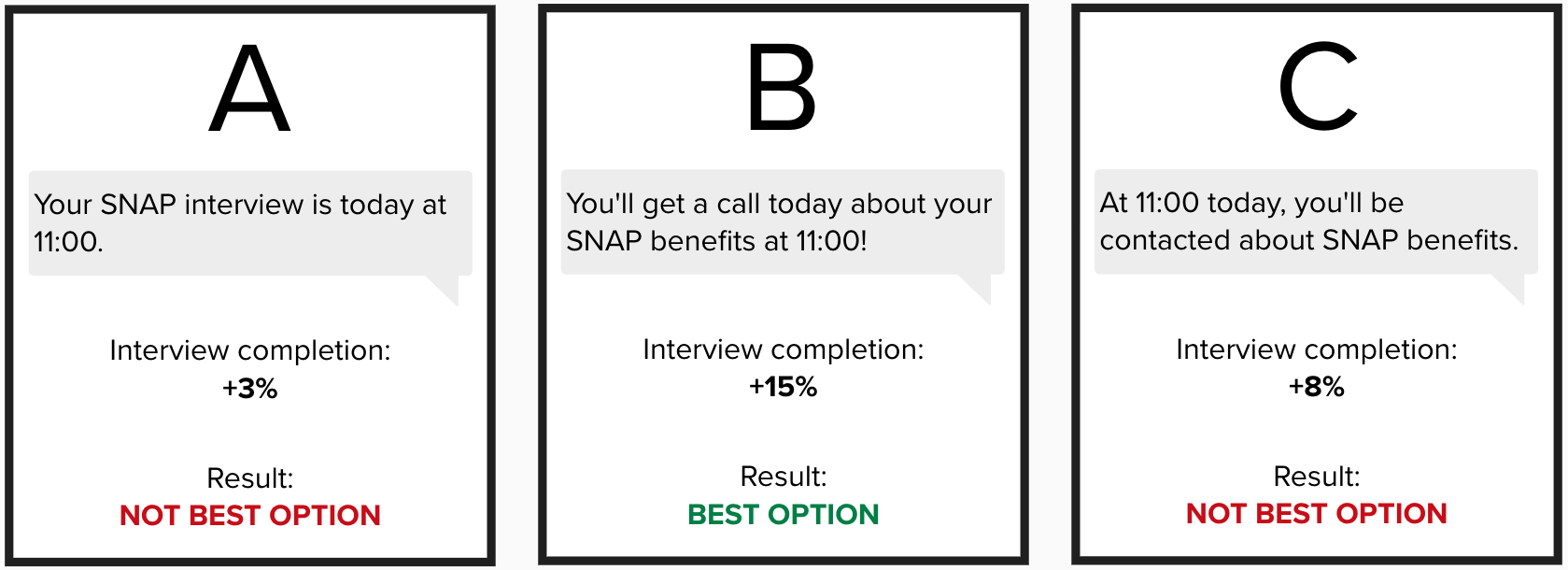
**Community based organizations (CBOs) or non-profits** – Examples include Navigator/Assister organizations, food banks, or advocate communities

**Potential recipients** – Content can be tested with potential recipients who are attending in-person interviews, or receiving assistance at a community organization

Testing and iteration **will take a significant amount of time**, but provides valuable feedback on the content itself. **Testing should be considered essential** to content development; however, it may not be feasible to test all messages with all groups. Potential recipients are often the hardest group to test with, so in many cases workers and CBOs can fill in the gaps.

## A/B Testing

If your processes allow it, A/B testing may be an option. In this scenario, two (or more) versions of the content are developed. Recipients **randomly** receive a version of the message, and output statistics are compared to determine which provided better results.



A/B testing requires **strong access to data** and flexible operational setup. But A/B testing provides the most significant feedback on the effectivity of the content, and can be used in an ongoing basis for improvement.

# Appendix A: WhatsApp

WhatsApp is an **Internet-based** messaging system that is more commonly used by members of migrant communities; outside of the United States, it has broad adoption. Because it is Internet-based, you **do not need a phone plan** to send and receive messages, making it a good candidate for recipients who may only have access to public Wi-Fi.

## Consent

Because WhatsApp is Internet-based, the FCC considers it in the **“unregulated area”**, meaning it is not subject to the TCPA. This does not alleviate all consent requirements, though. **Meta, the company that owns WhatsApp, has its own opt-in requirements[[11]](#footnote-11).**

In short, Meta requires that senders **get consent from potential recipients** before sending WhatsApp messages. This can happen via any method: oral, paper, digital, etc. This policy is enforced via spam reporting; **if too many recipients report the sender as spam,** WhatsApp may block or throttle their messages.

## Encryption

WhatsApp is end-to-end encrypted[[12]](#footnote-12); this is generally regarded as “secure” for the purposes of sending messages. This *may or may not* be secure enough for states to feel comfortable sending PII or PHI to the client; in general, it’s best practice **to keep private information out of messages**.

However, WhatsApp encryption is **far better than SMS**, which provides no encryption at all!

1. [FCC 03-1533](https://docs.fcc.gov/public/attachments/FCC-03-153A1.pdf) [↑](#footnote-ref-1)
2. [FCC DA 23-62](https://docs.fcc.gov/public/attachments/DA-23-62A1.pdf) [↑](#footnote-ref-2)
3. A great example of this is given in [Code for America’s guide to texting](https://files.codeforamerica.org/2022/11/02125302/Basics-of-Texting-Safety-Net-Clients-2022.pdf), which gives an example of opt-in from Minnesota. [↑](#footnote-ref-3)
4. [Reassigned Numbers Database](https://www.fcc.gov/reassigned-numbers-database) [↑](#footnote-ref-4)
5. [FCC Training on Public Benefits Texting](https://www.performance.gov/cx/life-experiences/facing-a-financial-shock/outputs/fcc-training/) (minute 7, also see description text) [↑](#footnote-ref-5)
6. [CBPP: FCC Ruling Allowing Automated Text Messaging Will Help State and Local Agencies With Unwinding Medicaid Continuous Coverage](https://www.cbpp.org/blog/fcc-ruling-allowing-automated-text-messaging-will-help-state-and-local-agencies-with-unwinding) [↑](#footnote-ref-6)
7. [FCC Regulatory Free Arena](https://www.fcc.gov/news-events/blog/2018/06/01/fcc-regulatory-free-arena) [↑](#footnote-ref-7)
8. [FCC Opt-out Ruling](https://www.fcc.gov/document/fcc-adopts-rules-empower-consumers-stop-robocalls-robotexts-0) [↑](#footnote-ref-8)
9. For additional evaluation guidance, see the [Beeck Center’s Digital Benefits Hub evaluation guidance](https://www.digitalbenefitshub.org/resources/text-to-connect-evaluation-of-your-text-messaging-program-to-reduce-snap-churn). [↑](#footnote-ref-9)
10. For additional information on content development, see the [Beeck Center’s Digital Benefits Hub content and strategy resource](https://www.digitalbenefitshub.org/resources/text-to-connect-strategy-content-for-using-text-message-outreach-to-reduce-snap-churn). [↑](#footnote-ref-10)
11. [WhatsApp Opt-In Requirements](https://faq.whatsapp.com/868507767645966) (Note: this page will not load on OMB machines) [↑](#footnote-ref-11)
12. [WhatsApp End-to-End Encryption](https://faq.whatsapp.com/820124435853543) (Note: this page will not load on OMB machines) While this resource is provided by Meta itself, WhatsApp encryption has also been verified (and criticized) by other sources: [Android Authority](https://www.androidauthority.com/whatsapp-encryption-safe-3087607/), [Ars Technica](https://arstechnica.com/gadgets/2021/09/whatsapp-end-to-end-encrypted-messages-arent-that-private-after-all/), [The Intercept](https://theintercept.com/2024/05/22/whatsapp-security-vulnerability-meta-israel-palestine/) [↑](#footnote-ref-12)