NNEDV

# Phone Communication With Survivors
# Best Practices

One of the more secure and easier methods of communicating with survivors is via phone calls. To ensure  privacy and safety, follow these best practices when communicating with survivors via traditional phones. For information about other ways of communicating with survivors, including using text, chat, video calls, and email, please see our Digital Services Toolkit.

## Calling Survivors

Before calling a survivor, have a conversation with them about if and when it is safe for you to call. Some survivors may have abusers who are monitoring phone calls. Some survivors may have privacy concerns as well, if they have not disclosed abuse to friends, family, roommates, or coworkers. So, it’s important to allow the survivor to determine the call back time and process.

## Leaving Messages and Voicemails

Before leaving a message with someone other than the survivor, or a voicemail, talk to the survivor about their safety and privacy needs, and what kind of information (if any) to leave in your message. Work with the survivor to choose options that best suit their current situation, and remember to check in with them regularly to see if their needs have changed.

If you have not been able to discuss safety issues before leaving a message with the survivor, leave a  vague message. You might decide to include your name, the reason you are calling, but not the name of your  organization or even your phone number. Your message could be: “Hello, this is [your name]. I’m returning your call from this morning. [If it’s vague enough, include about what.] You were asking for some information. You can call me back between the hours of 9-5, Monday through Friday.”

### Dropped Calls

Since many callers may be using cell phones, dropped calls may occur; or they may need to hang-up quickly for safety or privacy reasons. Ask the survivor ahead of time what protocol works best for them. Do they prefer that you call them back, or to have you wait for them to call you back? This is particularly important for hotline calls. Let the caller know what your program's practice is when a call is dropped; for example, you can't call them back, but they can call the hotline again at any time.

### Programs' Caller ID

Most phone carriers will allow you to block your number from showing up on the caller ID of the person receiving your call. You can also do this manually for each call by dialing *67 before you dial the number. Some smartphones offer this option in the settings, where you can turn the caller ID on or off.

If your phone system is set up to block your number on the caller ID, check it regularly to make sure that it still works. Upgrades and changes by the phone carrier or your smartphone could unblock the caller ID.

Some survivors may have their phone set up to reject calls from blocked numbers, and some survivors may have installed apps that can reveal numbers that are blocked. This may be a safety strategy to protect against harassment. If the person you are calling is using that feature, let them know about your organization's policy, and the reasons you block your caller ID (potential safety and privacy risks for some survivors). Then strategize with them about the best way to reach out.

Some programs, particularly those that are under a larger social service agency, may have a different organization associated with their phone number. Instead of the caller ID showing up as "domestic violence shelter" or "rape crisis center," it will say "Salvation Army" or something else, which may be safer or more private. Another option is to use a caller ID spoofing service to replace your program's number with an alternate number in the survivor's caller ID.

## Phone Systems & Safety

The type of phone systems your program uses will have an impact on privacy and safety as well. Your program may be using a traditional land-line phone system, a Voice over Internet Protocol (VoIP) phone system, and/or cell phones. One isn't more secure than the other, but depending on the phone system you are using, be aware of the privacy and safety risks that each system poses. Read more about using cell phones to communicate with survivors.

## Callers' Personally Identifying Information

Your program may be collecting identifying information about the people who call, even if you aren't doing so on purpose. Most phone systems now are designed to collect and store call history, caller ID, voicemail, transcribed messages, and more. How you collect, keep, and store survivors' personally identifying information can impact their safety and privacy, as well as your confidentiality obligations.

Some phone systems, particularly VoIP and mobile devices, offer the ability to translate voicemail messages into email or text messages. If your program wants to take advantage of this feature, keep in mind that you will also have to consider safety and privacy concerns for email and text messaging. While it may be harder for someone to intercept or accidently forward a voicemail message, it is much easier to intercept a text message on an advocate's personal cell phone or to forward an email that has a voicemail message attached.

If your phone system collects caller ID, voicemails, etc., you should have a policy detailing why that information is collected and how long that information is retained. It is best practice to keep the minimum amount of information necessary to meet the survivors needs (and your reporting requirements), and to only keep information for as long as you absolutely need it. Read our FAQs on Record Retention and Deletion for more information about handling personally identifying data.

Hotlines that promise anonymous calls are particularly obligated to ensure that callers are truly anonymous, which means not keeping callers' phone numbers. A person's phone number can be identifying since a reverse phone number lookup online can reveal who owns that phone number and even where they live.

Many phone carriers offer their customers access to call logs and other information through online accounts or billing records. When determining data retention policies, don't forget to consider access to these accounts. You may want to limit who on staff can access these accounts. When receiving bills, you may want a policy in which your program immediately destroys the portions of the bill that contain personally identifying information.

Hotline management systems may also collect survivors' personally identifying information. These systems should be set up to delete information about calls as soon as possible, and should never keep copies of the content of conversations. Also, while some systems offer to integrate with client databases, routinely or automatically collecting this information is unnecessary and goes against best practices for confidentiality. The level of detail about when and how frequently a survivor contacts you is generally not needed in order to provide quality services.

For more information about communicating with survivors using technology, see our Digital Services Toolkit, or contact Safety Net.

Supported by US DOJ-OVC Grant #2017-VF-GX-K030. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.