NNEDV

Using Mobile Phones to Communicate with Survivors: Policy & Practice Recommendations

Many domestic and sexual violence programs use mobile phones to communicate with survivors. While mobile phones offer convenience, privacy and safety issues need to be thoroughly considered. As with the use of any type of technology, it's important to have clear policies and procedures to outline proper use to maintain privacy for survivors and your program's confidentiality obligations.

NOTE: This document focuses on advocates' mobile phone use. Read more information on survivors' cell phone safety and privacy in our Survivors' Toolkit.

Purpose of Mobile Phone Use

Consider the reasons advocates within your program would be using mobile phones for work. These reasons will be the foundation to forming policies around advocates' mobile phone use. Some common reasons include being more easily accessible while out of the office, answering hotline calls from home, and texting with survivors if the survivor prefers it. Read more about texting with survivors in our Digital Services Toolkit.

Not all employees need a mobile phone for their work and advocates who have different roles may need a mobile phone for different reasons. The policy should reflect that. For example, an advocate who travels to meet with survivors may need to make phone calls and send text messages, while an advocate who does community outreach may need to access work email while out of the office.

Recommendations

- Policies should outline the purpose(s) of mobile phone use for work, and have a Mobile Phone Use agreement with each advocate.
- Policies should be clear about expectations of advocates' availability by phone when away from the office and supervisors should regularly check in about

work-life balance, boundaries, and signs of vicarious trauma or burnout.

Programs Should Provide the Mobile Phones

While there may be a substantial cost for both devices and voice/data plans, it is best practice for programs to provide mobile phones to advocates rather than ask advocates to use their own personal phones to communicate with survivors.

Risks when Advocates Use their Own Devices

There are serious risks to programs' confidentiality obligations, and potentially survivor safety concerns, when advocates use their own mobile phone to communicate with survivors.

If advocates' friends and family members have access to an advocate's phone, they could see survivor information in the contacts, email, or text messages. In addition, if the advocate's phone was part of a family plan, the account holder (which may not be the advocate) could have access to phone records and other details that could include survivor information, breaching confidentiality.

Another risk to advocate's using their own phones is if the phone is lost or stolen, the program may not be able to demand that data on a lost phone be remotely wiped, or if an advocate leaves the program, information on their personal phone will not be accessible to the program.

Benefits for Program-Issued Mobile Phones

Program-issued mobile phones enable programs to better ensure the security of devices, strengthen confidentiality practices, and support healthy work-life balance for advocates.

When programs own and manage a mobile phone, they can set up and have control over the phone and accounts associated with it. This includes the data on the device as well as data that is in the connected cloud accounts (Google account for an Android phone and iCloud for an iPhone.)

If a phone is stolen or lost or if a staff person using the phone leaves, the program can easily transfer it to another advocate, or wipe the device. Owning and having control over the mobile devices means that the program will have more security control over the accounts that are connected, apps that can be downloaded, or websites visited from the device.

Devices

Although older cell phones (flip phones or voice only cell phones) are still available, smartphones are widely available. If an advocate is only making phone calls or sending texts, an older cell phone may be more appropriate and safer. However, smartphones may be preferable because advocates can use apps such as maps or the internet. The downside is that smartphones have more privacy risks because of the apps that can be downloaded and the cloud-based accounts that are connected to the phone. Consider why staff would need a mobile phone and provide the type of mobile phone that would be most appropriate. If advocates are using smartphones, develop policies and agreements that addresses security and privacy risks.

Phone Security

Mobile phones should be set up by knowledgeable IT staff for enhanced security and should be checked by IT staff on a regular basis. The checkup should include needed updates, a scan for malware, a check of all installed apps, and any other security concerns. Additionally, you may consider implementing the following basic security measures:

- *Passcodes* - All phones should require a passcode, password, biometric factor, or other security measure to unlock the phone. Do not use the same passcode for every program phone, but supervisors or IT staff should always be able to unlock the phone in case an advocate cannot. All phones should automatically lock after a short time when not being used.
- *Antivirus and anti-malware apps* - All phones should have antivirus or anti-malware software or apps installed and updated regularly.

- *Remote wiping* - Programs should have the ability to remotely wipe the content of a phone that is lost or stolen.
- *Parental controls* - Programs should exercise caution when considering installing or enabling features that permit controlling or monitoring of the phone. These features should always be used with the advocate's informed consent and respect to privacy.

Smartphones and Cloud-Based Accounts

Most smartphones require an account to be connected to the phone. Generally, iPhones require an iCloud account and Android phones require a Google account. Depending on the type of phone, the manufacturer may also offer an account for the phone to offer different apps, manage security features, or store additional data. While phones connected to a cloud account may back up information from the phone by default, it is best that any personal information about a survivor not be backed up. This may mean turning off syncing of most services and apps.

Recommendations

- Do not use the same cloud account on more than one phone. Doing this will connect all the phones to one account, which means that some information, such as contacts or messages, could be shared among the phones.
- Minimize the amount of information synced to cloud accounts, particularly information regarding survivors. Most smartphones and apps allow users to determine which data, if any, is synced to the cloud or other connected devices. Check for and purge any survivor data from the backup regularly. Also check to make sure that updates to operating systems or apps have not reset these settings.
- Limit who has access to the cloud's account logs and information. Cloud accounts can reveal personal information about the user of the device, including the location of the phone and even messages sent through the phone.

Location Services and Apps

Phones should not have location sharing or tracking turned on without informed consent of the advocate. Some programs may want to track the location of a program-issued phone for the safety of the advocate or to locate a lost device. However, location tracking for the purpose of monitoring an advocate's location for employee management purposes is not appropriate.

If using location services for apps (such as Maps), advocates should understand the benefits and risks of using location services. Location history could be stored on the device or cloud accounts associated with the device or apps. Keeping location history could violate a survivor's privacy or become a safety issue if the advocate met with the survivor. Advocates might also be targeted by an abusive person and so should have their real-time location information protected.

Recommendations

- Phone location should not be stored in the history of the device and should be turned off or set to a less accurate setting if not needed by the advocate.
- When using location services for apps such as maps or navigation, the location history should not be stored. If this is not possible, it should be deleted regularly.
- Specific locations such as home, survivor meeting places, or work should not be saved to the app or phone.
- Turn off "geotagging" in camera apps, which will prevent the storing of location information in digital photos or videos.

Voicemail

Some phone systems offer the ability to receive an audio recording or a transcript of the voicemail in an email or text message. This creates a risk of interception or inappropriate access if the email or text is delivered to the mobile phone. Read more about Phone Communication with Survivors in our Digital Services Toolkit.

Recommendations

- Avoid automatically forwarding office voicemail to a mobile phone.
- If voicemails are forwarded, delete audio recordings, emails, and text messages of survivors' voicemails messages as soon as they have been listened to.
- Use a secure passcode for voicemail on a mobile phone.

Texting & Messaging Apps

Texting and messaging are other ways programs can use to connect with survivors. Messaging can increase access for some survivors, keep survivors engaged, and can be used to relay information when a survivor isn't able to talk on the phone. Read more about Texting with Survivors in our Digital Services Toolkit.

Recommendation

Delete messages as soon as possible from all devices as well as cloud accounts where messages could be stored.

Email

Depending on the advocate's role and work needs, they may need to access email while out of the office. Access to work email from a smartphone could create additional confidentiality risks. If access to email on a smartphone is necessary, ensure that confidentiality policies and practices include email on smartphones. Read more about Emailing with Survivors in our Digital Services Toolkit.

Remote Access to Files & VPN's

If staff need to access files from a phone (or another device such as a tablet or laptop) while away from the office, secure file sharing "cloud" services exist to help manage security. Look for "No-Knowledge" or "Zero-Knowledge" encryption options where the tech company itself cannot see the content of the files because they do not hold the encryption key – only the program does. Also, choose a service that allows you to control user-by-user access to the files so you can add or revoke access at any time.

Another option is to use a VPN (Virtual Private Network) from a reputable provider, which will provide a strong layer of security for the data that staff is sending and accessing. Bear in mind that a VPN won't protect the data from access or monitoring while the data is on the phone, but will increase data security while it is in transit. Read more in our handout, WiFi Safety & Privacy: Tips for Victim Service Agencies & Survivors.

Contacts, Call Logs & Text Logs

Minimize the amount of information saved on the phone. Your policies should include deleting information regularly, in most cases as soon as possible.

Recommendations

- Don't save survivor contact information in a mobile phone.
- All incoming and outgoing calls and texts should be purged regularly.
- If the phone has both internal memory and a memory card, save to only one and regularly delete from that. Saving to a memory card offers greater protection since a memory card can be removed and destroyed.
- Before getting rid of a phone or updating the phone to give to a new advocate, reset the phone to factory settings to clear any data that is on the phone.

Calendars

If the calendar on the phone includes appointments with survivors, schedule survivor information in a way that reduces the likelihood of it being identifying. Some calendar programs allow users to create multiple calendars. Consider creating a calendar for only appointments, which can be synced to the phone and then deleted when no longer needed.

Personal Accounts on Work Phones

Smartphones, and the apps installed on them, have the ability to have more than one account configured to it. Staff should not have personal accounts configured to a work phone. Having a personal account on the phone could lead to accidentally mixing survivor information with personal information or accounts. This also protects advocates' privacy, since personal information on a program-issued phone might make that information accessible to the program.

When Advocates Use Their Personal Mobile Phones

While it is our recommendation that programs provide mobile phones to advocates for work purposes, in the rare situation when advocates use their personal mobile phone to communicate with survivors it should be done so with specific consideration to privacy and safety.

Recommendations

- Advocates can use a virtual phone service and voicemail to contact a survivor, allowing the advocate to keep private their phone number.
- Alternatively, an advocate can prevent their number from showing in the receiver's Caller ID by either dialing *67 before dialing the number or turn off "Show My Caller ID" in the smartphone settings.
- Call logs and text message logs related to communication with survivors should be deleted immediately from the advocate's phone. Survivor's contact information should not be saved in the phone or the advocate's account.
- Programs might consider including some of the basic privacy and security practices described above in a Mobile Phone User Agreement.

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.