APRIL 2020

Alianza por la
Solidaridad
Member of **act:onaid**

REMOTE GBV SERVICE DELIVERY

Safety and Security Guidelines

PREPARED BY:

ALIANZA POR LA SOLIDARIDAD PALESTINE

GBV Protection amidst COVID crisis

In a crisis situation such as we encounter right now during the COVID-19 epidemic, when governments recommend „social distancing" to slow the spread of infection, technology is being used to connect to survivors of GBV. Communicating with survivors through technology comes with benefits and risks:

Communicating via email, text or online chats leaves a trail that might impact the personal safety of survivors of violence. Software being used or the history of text messages on the phone will reveal that a survivor is seeking help.

By sending messages when seeking help, the survivor loses his privacy since the message thread can be seen without their consent by others. Furthermore, there is the fear by the survivor of being recorded by a third party, which may result in blackmailing and exploitation situations.

When staff uses mobile devices to communicate with survivors, conversation threads and other related records reveal personally identifying information about the survivor.

Not only is it adamant that survivors are able to have a safe space when reaching case managers, organisations should also make sure that the counsellor, who is working from home, is able to ensure safe and private conditions when providing remote case management (e.g. having a room where she/he can work in privacy and uninterrupted by family members). If this is not the case, GBV case management should not be provided.

Case managers should also continue to have access to supervision and multi-sectorial case management coordination meetings to ensure the quality of services.

It should also be noted that using personal devices may severely impact the work-life balance of staff since they will be available for calls 24 hours a day. In an already stressful situation like this pandemic, the self-care of staff is of equal importance. Ideally, staff should have access to work phones so that they can adhere to off-duty times.

CASE MANAGEMENT MODALITIES IN THE COVID-19 SITUATION

These three steps should be followed when providing remote case management:

PREPARATION

Prepare your family and kids, explain the importance and the sensitivity of your work according to their age and understanding, explain to your kids that being busy and in a closed room is not related to neglect. In emergency situations like this one, other people need help, explain you will get back to them as soon as you can. Try to share responsibilities with your partner and elder kids, you may agree on a sign when you receive an emergency call so you can switch responsibilities.

VERIFY CONDITIONS

Verify that the survivor is in safe and secure conditions, inform her/him about the services and proceed with case management only if you receive informed consent.

If you want to schedule a session and you are sure that the phone belongs to the survivor and it is safe to text, ask if she/he is available for a talk. Do not mention that this is related to case management or mention your organisation's name.

In case you call the survivor, please first monitor if she/he sounds uncomfortable or if there is any background sound.

iF this is the case, please do not continue and ask the survivor to contact you when she/he is available through a missed-call, text message, or any other appropriate means of communication that you agreed on. Please re-evaluate their referral pathways and emergency plans, due to the current COVID situation and the resources available, take into consideration reduced working hours at courts, police station...etc.

Once the above mentioned measures are in place, please ask the following questions to confirm the safety and security conditions:

- Are you comfortable talking right now? Do you agree to continue this talk over the phone? Or do you prefer we schedule at a different time? Do you prefer a missed-call or text me when you are ready?

- Is this the right number to call? Do you prefer me to call any other alternative number?

- Are you taking the call from a room that can ensure privacy and confidentiality of the conversation?

- Do you think someone might walk in during our conversation? What do you advise as the best action to do if this happens?

- Ask again: Do you feel safe and have enough privacy for our conversation?

- Are you fine talking now? (Ask for consent repeatedly)

FINAL CONSIDERATIONS

Once the safety of the survivor is ascertained, the case management process can be started. It is important to assure the confidentiality of the survivor during all steps of case management.

Take the survivor through the case management steps and make sure that the survivor understands each of the steps (see the Interagency GBV Case Management Guidelines for further guidance).

Please bear in mind to make a remote session briefer than a face-to-face session since the survivor may have limited time to speak safely.

When ending the call, remind the survivor to delete signs of the call from the phone.

PANTICIPATE AND PLAN RESPONSES

Ensure safety measures are in place in case you get interrupted or in case the survivor does not feel safe anymore. Decide   with the survivors on the following scenarios:

- Someone asks what the survivor is doing and/or to whom they are talking to over the phone.

- Someone, such as the husband or father of the survivor or any other untrustworthy member in the household, answers the phone.

- The survivor starts not feeling safe anymore as someone may be listening and needs to stop the call.

- There is a need to talk to the survivor from an alternative phone number during the interview.

- Agree on a safe word or a code that you can use if the survivor feels unsafe or listened to (something simple such as discussing the weather, COVID-19 guidance, or any activities they participate in, etc.).

If the survivor does not sound comfortable and/or you hear any disturbing sound during the interview, please do not continue and give them an option to contact ou when they feel more comfortable speaking. Under such circumstances, never push for information.

SAFETY CONCERNS

If the survivor is scared for her/his safety and feels in danger, ask the following questions:

- Can you run for help?
- Are you in a locked room?
- Can you lock yourself away from the abuser?
- Is there anyone I can call for you?
- Shall we call the police?
- Is there a neighbour/friend you can reach?

DATA SAFETY

Ideally, paper files of the survivor should not be stored at the home of the case manager or counsellor. If the case workers fill out any forms during the interview, it is important to ensure the safe storage of any document with or without identifiable information.

Documents prepared during remote case management should be cared for in the same way as face-to-face case management. In such cases, please keep the information in a safe place with a locked drawer.

In case any electronic case management system is in place, please follow the agreed-upon data protection measures.

COMMUNICATION USING PHONES

When using the phone to communicate with a survivor, it is necessary to establish with them if and when it is safe for the counsellor to call, especially if the abuser is monitoring phone calls. The survivor should be able 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 on the phone of the survivor, talk to the survivor about their safety and privacy needs, and what kind of information (if any) to leave in your message. The survivor has the right to choose the best possible option, which should be assessed regularly to see if the needs have changed.
If there has not been an opportunity to discuss safety issues before leaving a message, this message should be vague and not give away any sensitive information to whoever might be listening. A sample of this
message could be: "Hello, this is [your name]. I'm returning your call from this morning. You were asking for some information. You can call me back between the hours of [..], Sunday through Thursday."

Dropped Calls

Some survivors may need to hang-up quickly for safety or privacy reasons. Discuss with a survivor at the first telephone call how you should respond to this, whether they prefer for you to call back or to wait for a call from you.

Storing Phone Numbers

Do not store the phone number of a survivor in your phone under her/his name, but use the survivor's ID code.

COMMUNICATION USING TEXT MESSAGES

Survivors and staff usually use cell-based texting or messaging apps when communicating through text messages. The most common messaging apps are Facebook Messenger, WhatsApp or Telegram among others. It is important to assess with the survivor individual safety risks and the device used to decide on which messaging platform best meets the needs of the survivor.

WhatsApp

WhatsApp is the most widely used mobile messaging app. It allows private individual and group chats and calls, and also offers end-to-end encryption so no third party can view the messages, and promises this security is automatic without turning on any additional settings. There is also a way to enable self-destructing messages.

WhatsApp makes it impossible to retrieve old chats on a new device, meaning that if an abuser takes the SIM out of the phone of a survivor of violence, the messages won't show up on the new phone. However, it is important to bear in mind that since Facebook bought the app in 2014, information can be shared with Facebook.

Telegram

Telegram allows the use of "secret chats" and promises "end-to-end encryption" which means that messages are unrecoverable, unlike common email or texting. Messages cannot be forwarded, and when you delete a message on your side, it instructs the message to be deleted on the recipient's side as well. If someone screenshots your message, you're notified. There is also a mechanism to set up a self-destruct timer before sending a message, forcing the message to destroy itself in a certain number of minutes after it appears on the recipient's screen. However, communicating in an encrypted way needs to be specifically turned on as a setting, which is something that beneficiaries need to be made aware of. It should also be explained that Telegram leaks metadata, which can show when the user was online and offline, who they are talking to and when they are using the app, making them vulnerable to stalking from the abuser.

It would be beneficial to use texting services that are not tied to one cell phone but to a texting platform, thus allowing more than one staff to manage text messages and to be able to adhere to a schedule and sign off after one's shift. Platforms used for message-based services should have strong privacy and security protocols to increase privacy for survivors.

Minimising Interception

1

When texting, both the sender and receiver has the history of the entire conversation, the date and time and perhaps even location, which can pose a great risk to a survivor's safety and privacy. Message history can also be revealed if the abusive person is monitoring the phone through physical access, monitoring software on the phone, or backups online.

Best practice:
If a survivor feels that the phone might be monitored, strategies need to be discussed, such as deleting the message history and not saving contact details such as the name of the organisation or counsellor in the phone.

Remind the survivor about cloud accounts such as iCloud or Google that may backup the messages or make them available on other devices.

If there are concerns that the device or account may be monitored, offer other options for more secure communications.

Prevent Impersonation

2

One risk when messaging with survivors is others impersonating and pretending to be the survivor. This is easily done, especially if the survivor does not have a password on the phone or the abusive person knows the password.

Best practice:

Establish a method to verify identity, which may include a previously agreed upon codeword or phrase.

Check in regularly with the survivor to make sure messaging is still a safe method of communication.

If either the counsellor or survivor becomes uncomfortable with messaging, check in by other methods, such as phone-to-phone.

Ensure Data Privacy

3

By using text messaging, essential information about the survivor is stored on the device of the counsellor, which can be accessed by family or friends. It is therefore not recommended that staff uses personal cell phones to text with survivors in order to ensure confidentiality.

Best practice:

Counsellors should not use their personal phones to message with survivors.

As little information as possible should be saved on the phone, which includes not saving survivors' full name, phone number, or other contact information. When the counselling period has ended, all contact information needs to be deleted from the phone.

Messages should be deleted regularly from the phone.

Do not offer to store or keep evidence for survivors. Discourage the sharing of pictures of abuse or forwarding abusive messages since counsellors should not become part of the chain of custody for evidence.

4
Set Survivor Expectations and Appropriate Staff Boundaries

Messaging allows the survivor to contact staff at any time, including after hours. In order to ensure the self-care of staff, it is necessary to establish boundaries with survivors. It should be discussed at what times the case manager can be reached and beneficiaries should have a clear expectation of when they will likely receive a response.

Best practice:

Set boundaries about work hours and availability with survivors when using messaging. Agree on the exceptionality of emergency situations.

Discuss survivors´ expectations in order to avoid frustration for both sides, clearly explain case manger's capabilities and your organizations limits.

GBV INFORMATION MANAGEMENT

Primero/GBVIMS+
can also be used as a remote supervision tool to review case files of staff.

Organisations could consider using Primero/GBVIMS+ which is similar to the GBVIMS as an inter-agency GBV case-management tool and is particularly useful in a situation such as COVID-19 when GBV service provision needs to be delivered remotely.

It allows for use in low and infrequent internet connectivity context, which may be the case if GBV caseworkers are based at home with no regular internet connection and it allows case managers to work paperless. Data collection can also be used without internet connection on mobile devices; in this case mobile devices require only a periodic access to the internet.

FOR MORE INFORMATION PLEASE CONSULT www.gbvims.com

Alianza por la Solidaridad

Member of **act!onaid**