Disclosure of Gender-based Violence in Humanitarian Crisis Settings

Guidance Note for Remote Service Provision

2022

Center for Human Rights, Gender and Migration
INSTITUTE FOR PUBLIC HEALTH AT WASHINGTON UNIVERSITY

Contents

Introduction

In 2022, the Center for Human Rights, Gender and Migration at Washington University's Institute for Public Health (CHRGM) published a report and practitioner's toolkit focused on the disclosure of gender-based violence (GBV) to service providers in humanitarian crisis settings.[1] As defined in this project, GBV "disclosure" is related to, but distinct from, more systematic, organization-driven "identification" efforts in these contexts. Instead, "disclosure" focuses on the experiences, perspectives, and needs of a survivor that may influence their decision or ability to come forward and speak. It is critical to understand facilitators and inhibitors of GBV disclosure in order to create safe opportunities for survivors to express their need for - and ultimately access - support and protection.

CHRGM's toolkit, *Gender-Based Violence Disclosure Toolkit: Responding to Gender-Based Violence Disclosure in Humanitarian Crisis Settings (2022),* offers service providers four modules of practical guidance for approaching the disclosure of GBV ethically and effectively.

This supplemental guidance note elaborates on approaches to GBV disclosure in the context of remote service provision. "Remote service provision" refers to services that are provided at distance, usually through some form of communications technology (e.g., telephone hotline, SMS or social media chat, video conferencing) instead of in person. While remote service provision for GBV-related support and general telehealth practice have existed for many years, the COVID-19 pandemic forced many more GBV-related service providers to find ways to work at distance from their clients, patients, and communities of concern.

Many major humanitarian agencies have developed platforms to facilitate safe remote service provision. For example, UNICEF has developed innovations like "virtual safe spaces" for adolescent girls to gather and access information about sexual and reproductive health, or "U-Report", a cellphone-based platform that enables anonymous exchange of GBV-related information.[2] Humanitarian agencies' tech-based interventions facilitate mobile and remote service provision – but they are generally proprietary and not available to unaffiliated service providers.

Thankfully, several organizations have issued helpful guidance about remote provision of GBV-related services in both humanitarian crisis and general contexts. This guidance addresses fundamental issues such as staff training and tech support, approaches for hotline-based response, safety planning for callers, confidentiality, and data security. They can be useful to many service providers across contexts and sectors. For example,

- International Rescue Committee, Guidelines for Mobile and Remote Gender-Based Violence (GBV) Service Delivery (2018)[3]
- Inter-Agency Standing Committee, Operational considerations for multisectoral mental health and psychosocial support programmes during the COVID-19 pandemic (2020)[4]
- UNICEF, Not just hotlines and mobile phones: GBV Service provision during COVID-19 (2020)[5]

- Gender-Based Violence Area of Responsibility (GBV AoR)[6] Helpdesk et al, COVID-19 Guidance on Remote GBV Services Focusing on Phone-based Case Management and Hotlines (2021)[7]
- National Network to End Domestic Violence, Safety Net Project: Exploring technology safety in the context of intimate partner violence, sexual assault, and violence against women – Digital services toolkit (2019, with additional COVID-19 updates)[8]

This guidance note does not duplicate or stand in for these resources. Instead, it draws from and builds upon them to highlight aspects specifically relevant to "GBV disclosure" in the context of remote service provision. It should be read in conjunction with CHRGM's GBV Disclosure Toolkit.

Choosing the Tool(s)

This section discusses the mundane but critical issue of choosing the right tools. How can the use of new technology for remote service provision affect survivors' willingness and ability to speak about their GBV-related experiences or needs? How can organizations and practitioners choose appropriate virtual tools and be best prepared for GBV disclosure via phone, social media, or other technologies? To what extent can an organization adapt communication methods based on the needs and preferences of diverse clients?

GBV service providers should select and use the most appropriate technology based on survivors' needs and technology support available to staff. Much can be learned from practitioners providing hotline support or services focused on domestic or intimate partner violence. For example, the National Network to End Domestic Violence (NNEDV) published an extensive online resource: the **Digital Services Toolkit**.[9] Among its modules, the Toolkit includes *Best Practices Principles for Digital Services, a Step-by-Step Guide to Choosing Tools for Digital Services*, and specific tips for safe texting, phone calls, video calls, and other means of communication with survivors.[10]

Further, mental health and psychosocial support experts have identified several promising "technology practices" for remote service provision, including performing a technology check in with the survivor, reassuring patient of privacy and technology security[11], using platforms that guarantee confidentiality on both ends[12], recommending that patients use private WiFi or hard-wired connection rather than connecting to public WiFi[13], and establishing standard operating procedures to develop contingency plans for service disruptions due to technology problems[14].

> **Practice tip from the National Network to End Domestic Violence[15]: Adapting communication tools for different survivors' needs and preferences**
>
> … It's important to be survivor-centered when communicating remotely. The best tool to use is the one that works best for the survivor you are working with. One survivor may prefer to talk on the telephone while they are taking a walk outside. Another may prefer text or chat because it is a quiet way to communicate if the abuser is nearby. Someone else may prefer video because they like the sense of personal connection.
>
> To help a survivor decide what tool is best for them, discuss the safety of their devices and surroundings. Offer a number of ways to communicate, including a phone call, the audio-only option in the web conferencing service, online chat, or text messaging. Once you've helped with the privacy and safety planning process and provided options for communication, respect their choice about which tool best meets their needs. Prepare tips and information to share with survivors about how to use the various tools you have available.

Digital Divide(s)

When shifting to remote service provision via phone, social media, or other digital platform, one key consideration is *access*: *Who can or will actually use the new method of engagement*?

While cell phones are used by people across income levels in many parts of the world, there are still several disparities to consider. For example, women and girls in many parts of the world have less access to cell phones and smart phones as compared to their male counterparts. This "digital divide" has implications for choosing modes of communication and service provision related to gender-based violence. *If survivors have trouble accessing remote services, they will also miss opportunities to disclose GBV-related needs to providers who can help.*

Gender and the "digital divide"

"Across low- and middle-income countries, the underlying gender gap in mobile ownership remains largely unchanged. Women are still seven percent less likely than men to own a mobile phone. The 372 million women still without a mobile phone are proving difficult to reach. The top barriers to mobile ownership are affordability, literacy and digital skills and safety and security."

"The gender gap in smartphone ownership has widened slightly. Over the past five years, the gender gap in smartphone ownership had been reducing year on year across low- and middle income countries, from 20 per cent in 2017 to 16 per cent in 2020. Women are now 18 percent less likely than men to own a smartphone, which translates into 315 million fewer women than men owning a smartphone. This year's increase has been driven by an increase in the smartphone gender gap in South Asia, as well as a continued increase in the smartphone gender gap in Sub Saharan Africa. However, once women own a smartphone, their awareness and use of mobile internet is almost on par with men."

GSMA, *The Mobile Gender Gap Report*, 2022[16]

Case study: Lebanon

In a study led by the International Rescue Committee (IRC) in Lebanon, one-third of female respondents reported device ownership, and most women report that they share devices with intimate partners, parents or in-laws. Moreover, only 17% of adolescent girls report ownership of a device. These results suggest that the majority of women and girls participating in the study may use devices that can be monitored or controlled by others, limiting their comfort with discussing GBV-related concerns and potentially putting their safety at risk. A gender analysis broadens understanding of women and girls' access to technology and other services in a given context. [17]

Other important tech access disparities to consider include (individually or intersectionally):

- **Urban v. rural communities**, as there may be differences in cell tower or internet reliability;
- **Age-related differences**, as older people may be less familiar with social media or new technologies, or young people may lack cell phones or private spaces of their own;
- **Literacy levels or language barriers** that may affect ability to respond to SMS- or other text-based communications, or to engage through modalities that do not support third party interpretation;
- **Socio-economic disparities**, which can influence access to necessary equipment (phones, computers) or the ability to afford costs associated with text messaging or cellular data / airtime;
- **Displacement-related barriers**, such as loss of normal phone or computer access, reduced income to pay for airtime, lack of private or reliable space while in rapid movement or refugee camp, and cultural / linguistic barriers due to distance from homeland.

Service providers are increasingly using new technologies to remotely serve persons of concern in humanitarian crisis settings – particularly in light of the COVID-19 pandemic, which introduced numerous restrictions on movement and use of space. Pandemic aside, war, natural disaster, and displacement can exacerbate challenges or disparities in survivors' access, control and use of phones and other communication devices.[18]

Practice Points: Maximizing access and engagement

Choice of technology can affect GBV disclosure. A first step in creating an enabling remote environment is to ensure that individuals can and will use an available mode of engagement. As noted above, some survivors may prefer to speak by phone while some may prefer silent texting. Here are some basic questions to consider when choosing tools for remote service provision[19]:

- What kinds of technology does the population have access to, particularly women and girls? What about the most marginalized individuals? What single or intersecting vulnerabilities affect access?
- Is there a phone network and electricity? How stable are they? What area do they cover?
- Is there the option of a toll-free number, or other strategies for the provider (rather than the survivor) to carry the cost of the call?
- Is it possible to access a conference call function (to support translation, connecting with supervisors, referral partners, etc.)?
- What are some of the anticipated safety and privacy issues women and girls may face? What concerns exist about perpetrator backlash? What steps need to be put in place to manage these safety and privacy issues?
- If individuals of concern do not have access to phones, are there places in their community where they would feel comfortable going to make a call? Is this movement possible at this time?

- Will people of different ages have particular challenges in using a remote case management service? How can these challenges be addressed safely and in age-appropriate ways?
- If services are offered to new clients, what is the best and safest way to advertise the services to the population of concern?
- What remote service technologies are most likely to safely reach other "invisible", marginalized, or extremely vulnerable populations (e.g., unhoused persons, individuals of diverse sexual orientation or gender identity / expression, survivors of trafficking)?
- When necessary, how can mobile, in-person service provision be arranged for individuals who cannot engage remotely?

Reflection on the above questions can help a team develop the best possible approach for remove service provision. In addition, it is important to ensure that:

- Options for remote service provision (e.g. via telephone, smartphone, computers, videoconferencing or chat applications) are available to, and easy to use for, both the service provider and the GBV survivor. Where possible, GBV survivors should be able to choose their means of engagement.
- There is a clear plan and process for covering any costs of remote interaction (text message charges, airtime for cellular data, etc.);
- Staff and any other relevant practitioners are properly trained on any new technologies or systems required for remote service delivery;
- The service team monitors and evaluates its reach into diverse communities, adjusting remote methods as needed.

Video-Conferencing Platforms

Video-conferencing provides the benefit of visual cues that can help promote rapport while also offering clues as to survivors' emotional responses and the safety of their surroundings. These insights can be critical when creating an environment in which GBV disclosure is possible. Though several video-conferencing platforms existed prior to the COVID-19 pandemic, there has been an explosion in the number of options available today. They vary in terms of functionality, cost, and security. When choosing a videoconferencing platform for remote service provision with GBV survivors, key features to look for include:

- Simplicity of interface, to accommodate diverse levels of technological and language literacy;
- Ability to use platform without complicated registration process, application download, or digital paper-trail (eg, generation of emails, ads, or other notifications);
- End-to-end encryption of video and text chat, though this may require paid subscription or other institutional arrangement for some platforms;
- Ability to access video chat by cellphone dial in;
- Text chat feature, in case survivor needs to communicate silently for entire or portion of the call;

- Capability for both one-on-one and group video chat, to have option of group discussion or interpreter participation;
- Ability to enable encrypted sign language captioning if needed;
- Ability to disable any built-in recording function (as recording and storage of recorded files often pose security challenges).

In 2020, the National Network to End Domestic Violence (NNEDV) compiled a comparison chart featuring key videoconferencing platforms that may be of interest to service providers.[20] A summary version of the chart is included in Annex I for purposes of illustration – it should be noted that platforms may have evolved. Functions, ownership, and privacy policies should be checked regularly for *any* digital tools used in a service provision context.

Practice Points: Preparing to video-conference GBV survivors (and others)

As part of its "Digital Services Toolkit", the National Network to End Domestic Violence (NNEDV) issued *General Best Practices for Digital Services*[21] and *Best Practices for Using Zoom: Safety, Privacy and Confidentially Considerations in the COVID-19 Pandemic*.[22] NNEDV offers the following key points for use of videoconferencing platforms (edited for length and clarity)[23]:

- Talk with survivors about the safety of their surroundings when videoconferencing. Depending on where they are, their conversations could be overheard by the abusive partner or someone they have not disclosed the abuse to previously.
    - Before the call or early into it, parties should agree on a "safety password" that the client / survivor can use if they need to stop talking in the course of a meeting. The password should be one that would not normally be used in the conversation but also that does not arouse suspicion if overheard.
    - If the client / survivor says the safety password during the meeting, both parties can make a "safe switch": The service provider can take on a different role or the parties can simply change the line of conversation (e.g,, about school or COVID or anything that would deflect suspicion).
- At the start of the virtual visit, disable recording to avoid security challenges.
- Check in with the survivor regularly to see if videoconferencing is still comfortable and feels safe. Offer other ways to communicate, including the audio-only option in the web conferencing service, a phone call, online chat, or in-person.
- Create handouts or tips on how survivors can access the video conferencing service.
- Test the technology to make sure it works properly before meeting with survivors.
- Notes regarding specific needs:
    - If a survivor is located in a geographic region where internet coverage is weak, video conferencing may not be the best method of connecting.
    - If a survivor has a disability and uses assistive technology, their assistive tech may not be compatible with the video conferencing platform, or they may not be able to utilize all of the features the video conferencing program offers.
    - If interpretation is needed, identify qualified interpreters for videoconferencing in advance and ensure that they can and know how to use the videoconferencing platform.

Using Social Media

For many cell phone and smart phone users, social media applications are an important way of staying in touch with friends and family. But can they be safely and effectively used in service provision? The answer is, it depends. Two key considerations are security and functionality.

Security. Messaging applications have different levels of data security. End-to-end encryption of messaging content, which prevents access by parties other than the sender and intended recipient, is increasingly the industry standard. A 2019 survey comparing security features of leading chat applications produced the table below. While potentially outdated, it may still help providers identify specific security features important to their work.[24]

Messaging App	End-to-end encryption	Encryption in Transit	Private key not accessible by provider	Deleted from Server	Self-Destruct Messages	Open-Source	Password lock	Verification SMS/Email	Screenshot detection	Two-step Verification	Remote logout	Remotely Wipe Messages	Account self-destruct	Free
Confide	✓							✓						
CoverMe	✓				✓							✓		
Dust	✓			✓	✓				✓					✓
Hangouts		✓												✓
iMessage	✓		✓	✓	✓									✓
Line	✓							✓						✓
Messenger	✓(optional)	✓			✓									✓
Signal	✓				✓	✓	✓							✓
Skype	✓(optional)	✓												✓
Slack		✓												✓
Snapchat	✓													✓
Telegram	✓(optional)	✓	✓		✓	✓	✓			✓	✓		✓	✓
Threema	✓													
Viber	✓		✓	✓	✓		✓							✓
WeChat														✓
WhatsApp	✓		✓				✓	✓				✓		✓
Wickr Me	✓								✓					

Apps are sorted alphabetically

Source: J. Botha, C. van 't Wout, L. Leenen. (2019). *A Comparison of Chat Applications in Terms of Security and Privacy.*

Finally, as with video-conferencing applications, ownership and privacy policies of social media platforms can change over time. It is critical to check for product updates regularly in case any changes compromise user privacy and security.

Functionality. Service providers seeking to use social media or other messaging platforms to communicate with clients and communities remotely may need the tool to do different things.

The following table highlights a few of the most commonly used messaging applications, all of which have the following functions: Text messaging, group chats, voice memos, phone calls, and video calls. Users can also share contact information, location, and certain kinds of files. The table below notes their additional functions, as well as more detail about their different security-related features. *It should be noted that this guidance note does not endorse any specific social media platform or application.*

Major social media messaging platforms: Additional functions and security feature summary	
Application / Owner / Website	Additional function and security features (non-exhaustive)
Facebook Messenger Owned by Meta (Facebook family) https://www.messenger.com/	Additional functions: 'Stories' sharing; group video calls; "Watch together" media viewing; stickers. Security: End-to-end encryption is opt-in only. Block unwanted contact. Secure the app with devise passcode, fingerprint, or facial recognition.
Signal Owned by Signal Technology Foundation https://signal.org/en/	Additional functions: 'Stories' sharing; group video calls; note to self; stickers, reactions. Security: Automatic end-to-end encryption for all messages, calls (including group calls), shared content, user information, and chat metadata. App can be secured with passcode, fingerprint, or facial recognition. Disappearing messages. "Delete for everyone" within 3 hours. "View-once media." On Android phones, incognito keyboard can be activated so phone does not retain memory of typed words. No user tracking, no ads. *Additional advanced options available, see website.*
Telegram Owned by Pavel Durov https://telegram.org/	Additional functions: Creation of large groups or 'channels for broadcasting to unlimited audiences'; live streaming to group audience. Security: "Secret chat" function allows for end-to-end encryption, timed message "self-destruction", prevention of message forwarding, and "delete for all" option. App can be secured with 2-Factor identification, a passcode, or facial recognition.
Viber Owned by Rakuten Viber https://www.viber.com/en/	Additional functions: Group video call; Create / join 'Communities' with similar interests; 'Stories' sharing; edit and delete "seen" messages; stickers. Security: End-to-end encryption of chat messages by default. Send disappearing messages. "Delete for all" option. Notification in case of chat screenshot. Chat without exposing phone number. Hidden chat function. No sale of user information, no ads.
WhatsApp Owned by Meta (Facebook family) https://www.whatsapp.com/	Additional functions: 'Stories' sharing; group audio / video calls; stickers. Security: End-to-end encryption of chat, calls, and all shared content. "Delete for me" option at any time, "Delete for everyone" within one hour. Option for message "self-destruct" after 7 days. Note 2019 hack and ongoing concerns over Meta's access to chat / user metadata and use for advertising purposes.

One attraction of many social media applications is the ability to create "group chats". When used on a secure platform and with clear ground rules, group chats may be a useful way to disseminate information about service provision generally as well as build solidarity and mutual support among a community or set of individuals. However, "group chats" should only be considered where one can ensure encryption of group chat content, participants, and metadata; members' adherence to clear rules about conduct, content, and confidentiality; and close moderation of group membership and the chat itself.

Practice Points: Choosing and preparing to use a digital platform, including social media

The following practice tips focus on safe choice and use of devices and communication platforms[25]:

- Where possible, staff / providers should not use personal devices for work – ideally, institutional phones should be provided for exclusive work use. Providers should not mingle personal and professional data on the devices.
- Only download apps that are necessary for work.
- Put a passcode on work devices.
- Install security updates and download anti-malware protection on all devices.
- Review the privacy and security settings on the device and in each app.
- Do not use public Wi-Fi if accessing client information or other sensitive information. Instead, use a secure network or VPN to connect with the office or to share files. Also, consider using a secure cloud-based file-sharing system.
- Limit apps' access to location, contacts, and other potentially sensitive information.
- Ensure that all call participants sign out of their accounts and/or close the program every time they step away from their device.
- Avoid standard cell phone text messaging with participants as it is more vulnerable to paper trails and security concerns.
- Research and consult community members to understand who uses which social media applications so you understand which tools would be most useful for remote service provision.
- Insecure or ad-based social media systems like Facebook Messenger should also be avoided. Instead, platforms that offer safety features like end-to-end encryption, "zero knowledge" encryption, and/or two-factor authentication should be used.
- If possible, providers should use platforms that do not require the participants to create an account or profile.
- Use of "group chats" may be beneficial for information dissemination and community building, but should only be undertaken where security and respect can be ensured. Adherence to clear ground rules and close moderation are essential.
- Whatever platforms or applications a team chooses, it is important to regularly check for changes in ownership and updates to the privacy policy.

The Remote Interaction: Safety, rapport, and responding to disclosure

As practitioners have long understood and as CHRGM's recent research confirms, an enabling environment can help GBV survivors feel comfortable speaking about their GBV experiences or needs. CHRGM's practice toolkit, *Gender-Based Violence Disclosure Toolkit: Responding to Gender-Based Violence Disclosure in Humanitarian Crisis Settings*, provides in-depth practical guidance for creating these environments under normal, face-to-face circumstances.[26] *Remote* service provision poses new challenges. In addition to choosing appropriate technology and platforms (discussed above), key ingredients for an enabling remote environment include somehow ensuring safety and building rapport despite physical distance.

Safety

Survivors need to feel safe in order to disclosure their GBV-related experiences or needs. One aspect of safety is literal – are they physically safe to speak with someone at that moment?

In some cases, it may be possible to make safety preparations. The GBV AoR provides the following helpful suggestions[27]:

- Work with client / survivor to determine safe call times and modalities;
- Ensure that all parties to a call receive training on how to delete texts and call history.
- Arrange for the client or survivor to initiate the call to the service provider. If they cannot afford airtime or do not want traces of the outgoing call on their device, determine if it is safe for them to text or make a "flash" call to signal readiness to be called back.

Of course, not all interactions can be scheduled – or sometimes circumstances change and scheduled times may no longer be safe. Once a meeting starts, it is critical to assess safety in that moment.

Practice points: Assessing safety during a call

One common approach for phone-based meetings is to ask the client or survivor certain safety assessment questions. These should generally be "Yes/No" questions that no one but the caller can hear.[28] The following suggestions are adapted from phone-based guidance issued by the GBV AoR guidance and International Rescue Committee[29]:

- Are you comfortable talking right now? If not, do you prefer we re-schedule? Or would you like to missed-call or text me when you are ready?
- Is this the best number to call? Or do you prefer I call a different number?
- Are you taking this call from a room where we can have a private, confidential conversation?
- Do you think someone might walk in during our conversation?
    - If the answer is yes, advise the client / survivor to use a "safety password" that they can use if they need to stop talking or if they are in danger. Ideally, this should be arranged at the before or at the beginning of a first meeting so it is understood for any subsequent conversations. Check that this has been done and the client / survivor remembers the password. See "*Practice Points: Preparing to video conference with GBV survivors (and others),* above, and make a "safe switch" if the password is used.
- If we are interrupted or if you need to hang up for a moment, would you like to reconnect? If so, how?
- Do you feel safe and have enough privacy to talk now?

Some, though not all, of these safety assessment questions may work for video-conference. While safety guidance for video-based service provision is limited, here are some key ideas to consider for video meetings (supplementing early *Practice Pointers: Preparing to video-conference with GBV survivors (and others),* above):

- Conduct safety assessment at the start of the meeting. As with phone-based meetings, agree on a "safety password" and "safe switch" process. One additional possibility that video conferencing allows is use of a silent "safety gesture" in case the client / survivor prefers her signal to be seen and not heard. For example, see "Signal for Help" from the Canadian Women's Foundation.[30] As with a verbal safety password, a physical safety gesture should be something not likely used in the normal course of conversation.
- Service providers should limit how identifiable they are to unintended or unexpected viewers. For example, they might take the call with a neutral background that does not indicate who they are or where they work. Similarly, if the video conferencing platform indicates parties' names, service providers should consider renaming themselves just using their first names, in case an abuser or other person sees them and is curious about their identity.
- If a conversation must be paused for a time, use the chat box with caution. Even if the survivor has indicated she is comfortable typing in the chat box, it is critical that the client / survivor is also able to delete chat contents immediately if needed, or to hang up.

Rapport

As many practitioners working with GBV survivors know, rapport is essential to GBV disclosure. CHRGM's research report and toolkit delve into concepts and practical approaches for building sufficient rapport with different survivors in different contexts.[31] This section highlights two major elements of rapport-building: privacy and earning trust. It proposes ways they can be approached in remote service provision.

Privacy. Privacy is related to safety: if a conversation is not overheard, it cannot be shared elsewhere. However, privacy and safety are not the same thing. For example, a survivor may

have *safety* if the only other person in the room is her seven year old daughter – but she may still hesitate to speak about GBV because she does not have *privacy*. Like safety, privacy is critical to enabling GBV disclosure.

Both provider and client need a private space where they can speak without being watched or overheard. During the COVID-19 pandemic, staff of some organizations were still able to work in private rooms at the organization's office. However, many staff pivoted to taking calls from home. In both cases, it is imperative that staff have a reliably private space to conduct calls and remote support provision so their conversations with GBV survivors are not overheard or interrupted.[32]

For clients or callers (in case of hotline, for example), it may be harder to find private space to speak with service providers, especially in cases of intimate partner violence or in crowded shelters or camps. Where a client does not have a safe, private place in their home, it may be worth exploring whether there are other safe spaces available where they can go to make a call – for example, a women's shelter, a safe space for women and girls, the home of a trusted community member, a local clinic or pharmacy, or even places of worship. In some cases, organizations might be able to arrange safe access to these borrowed spaces.

Earning trust and establishing rapport. As many practitioners well know, and as CHRGM's recent research clarified, GBV disclosure largely depends on trust. Trust that the person listening will not judge. Trust that confidentiality will be respected. Trust that the person listening can and will help. Establishing sufficient rapport is part of earning this trust and is thus essential for enabling GBV disclosure by survivors.

Practice Points: General guidance for establishing rapport as service providers

The below table, from CHRGM's *Gender-based Violence Disclosure Toolkit: Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings* captures ways to earn trust and establish rapport in a service provision context.

Establishing Rapport: Dos and Don'ts for providers who may receive GBV disclosure	
Things to do	**Things not to do**
Always show empathy and compassion.	Don't judge or blame a survivor for anything that happened to them. Remember that your own life experiences and background may influence how you view or interpret someone else's experiences and behaviour. Never criticize, challenge or question an individual if details in their story change.
Always explain confidentiality and any limits to confidentiality at the beginning of an interview or meeting.	Never ask someone about GBV in the presence of a partner, family member or friend.
Always maintain confidentiality.	Don't speak openly with colleagues about a case or whisper right after an individual shares sensitive information with you. This can erode trust and create anxiety. Don't bring up GBV or sensitive information on the phone or Zoom unless you have verified that all parties are in a private, confidential space.
Practice active listening, including making eye contact, being attentive when the person is speaking, and ensuring you are not distracted.	Avoid body language that conveys disbelief or irritation, such as crossing your arms or certain facial expressions. Do not check your phone while you are meeting with someone, unless it is necessary to help explain something.
Show that you believe the survivor's story and thank them for having the courage to share it.	Never push someone to talk if they are uncomfortable or are not ready. Instead, reassure them that they can talk to you later or refer them to someone else who can help.
Be honest, transparent and patient.	Do not ask unnecessary questions that are outside the scope of the conversation or your mandate.
Build the survivor's self-esteem by affirming their feelings, desires and expressions.	Do not take any action without the consent of the survivor.
Learn relevant colloquial or euphemistic expressions for sexual acts or anatomy.	Do not make assumptions about how a survivor is feeling after a disclosure; even if they appear calm, they may be distressed.

Source: CHRGM, Center for Human Rights, Gender and Migration, "Gender-based Violence Disclosure Toolkit: Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings." (2022)

Specific challenges to rapport-building can arise in the context of remote service provision. In addition to addressing a survivor's possible discomfort with the communication platform or safety concerns addressed above, it can be difficult to pick up on non-verbal emotional cues or to signal warmth and care over a phone or digital platform. In remove service provision, non-verbal communication is still extremely important – but it is different than when people are physically together. The GBV AoR reminds that without being able to see each other, parties

communicating by phone cannot rely on eye contact, facial expressions or other physical communication. Instead, each party's voice and speaking patterns (e.g., tone, breath, pauses, speaking pace, degree of calm) become more important signals to the other person.[33] Video-conferencing, fortunately, does allow for certain visual cues (e.g., facial expression).

Practice points: Building rapport remotely

Much about remote rapport building can be learned from telehealth service providers specializing in remote counseling or hotline staff working with survivors of intimate partner violence. Many have developed helpful strategies in communicating with survivors or clients they cannot see or cannot sit with in person. Below are some practice points for building rapport via phone calls, video-conferencing, and text messaging, adapted from GBV AoR guidance.[34]

Building trust and rapport by phone: Tips from hotline practice	
Dos for answering calls	Don'ts for answering calls
• Let the phone ring a few times before answering. This will give the survivor time to relax. This may be the first time they have contacted the hotline or disclosed the abuse to another person, so they may be feeling very anxious. • Have an opening statement to help put the survivor at ease e.g. "Hello, this is [your name or name of organization or hotline, whatever is most appropriate]. How can I help you?" • If the survivor offers their name, use it to help build trust. • You may tell the survivor your first name if they are very anxious. • Assure the survivor that the Hotline is confidential, if this is appropriate, but ensure to explain any associated risks. • If you cannot hear or understand the survivor, do not be afraid to gently let them know. • Pause often to give the survivor space to talk. Remember that it may be the first time that they have had an opportunity to speak about the abuse, or they may not be used to seeking support on the phone. • Use active listening skills, making acknowledging sounds when the survivor speaks. • Where appropriate, provide grounding and relaxation techniques. • Be aware of personal boundaries and holding them.	• Do not ask for the survivor's name unless you need it for follow-up or referral. • Do not talk too much, a lot of the work on a hotline is listening. • Never give out referral or any other type of information you are not certain of. • Do not overload the survivor with too much information. If they are upset during the call it may be more appropriate to focus on listening, rather than giving information. • Do not use "recording" functions unless absolutely necessary, as recording and automatic storage of recorded files to the platform may compromise security and confidentiality. • Do not share your personal contact information. • Never give out or take calls from survivors on your personal phone.

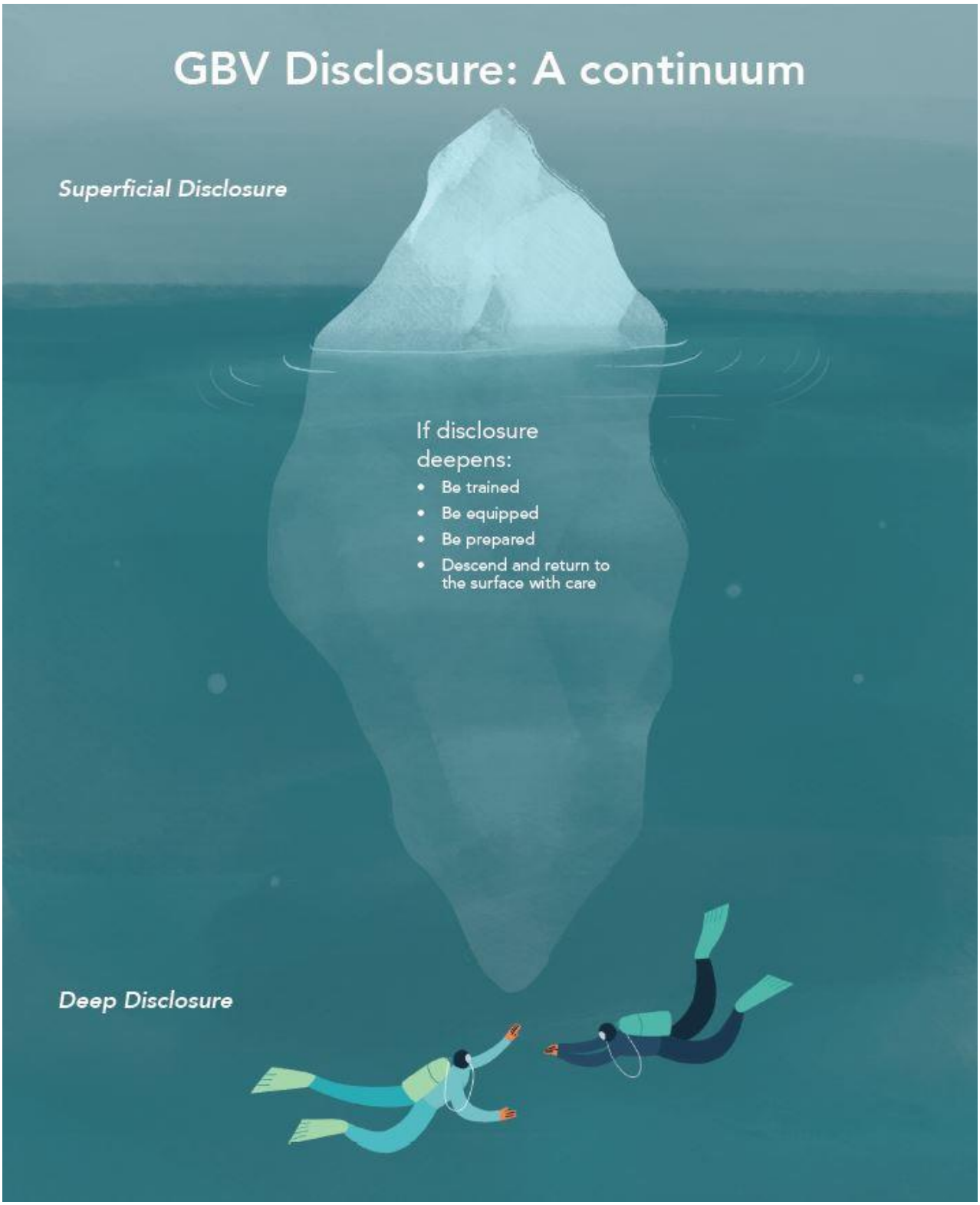
Practice points: Specific tips for building rapport over video-conference

With the COVID-19 pandemic, use of video-conferencing platforms like Zoom and Microsoft Teams has greatly increased in the context of remote service provision, including with GBV survivors. While video conferencing can offer more visual cues than interactions via phone, email, text or chat, it can still be challenging to develop sufficient rapport to enable GBV disclosure. Below are some tips to consider.

- Service providers should ideally keep their camera is on, ensuring that their image is clear and well-lit. This can help the survivor see supportive facial expressions, recognize someone they trust (if parties have met before), and even feel sure that a question or comment has ended. Sometimes people even enjoy meeting a wandering pet in the background!
- It is helpful if a survivor keeps her/their camera on for a video call, as well, since visual cues as to their own emotional response or physical surroundings are valuable. However, survivors may not feel comfortable with the camera on for different reasons. Make sure they know the decision is theirs – and that they can turn their camera on and off as they wish.
- If interpreters or others will participate in the conversation, be sure the survivor knows and consents to this in advance. It can be helpful to have all cameras on at the start of the meeting for greetings so the survivor knows who is "in the room." Once the call has started, others can offer to turn their cameras off to minimize distraction, unless the survivor wishes otherwise or there are other important reasons to keep everyone visible.
- Note: There may be good reason to turn one or more cameras off (e.g., low bandwith, concern over attracting attention of others, etc.). Check with the survivor for their thoughts and adjust according to comfort and safety needs.

Responding to disclosure

GBV disclosure can come be shallow or it can be deep. It can be a one-time event or it can be an ongoing, deepening process. It almost always needs time. Except for emergency situations, as in many hotline situations, it can help to offer ongoing contact where possible so that survivors can develop sufficient trust over time, despite any potential awkwardness of communicating through a device or screen.



Source: Center for Human Rights, Gender and Migration, "Gender-based Violence Disclosure Toolkit: Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings." (2022)

When GBV disclosure *does* happen, it is critical that service providers are prepare to respond empathetically and effectively. The CHRGM toolkit outlines key practices to consider – these are relevant even in the context of remote service provision:

- Remain calm.
- Let the person speak freely and tell their story in their own way and in their own time.
- Use active listening skills to show you are present, empathetic, non-judgmental and supportive and are able to listen to, hear and respond with compassion to what they are saying.
- Communicate that you believe them.
- Communicate that you are sorry for what has happened to them.
- Acknowledge how difficult it must have been for them to disclose, and reassure them that it was the right thing to do.
- Take steps to support the survivor's immediate safety and well-being, including through providing psychological first aid if you are properly trained to do so.
- Provide the survivor with helpful information to help them understand what has happened, what effects they may experience, and what services and supports are available to address their needs and promote their well-being.
- Help the survivor decide what to do next, and provide information and make referrals for additional care, support and protection for survivors who consent to referral. Make sure to communicate clearly about potential delays and waiting times for services where they exist, so that a survivor has realistic expectations about receiving support.

Practice points: Making safe, effective referral

A critical aspect of ethical, effective response to GBV disclosure is making sure the survivor gets the support they need. Many times, this was their motivation to speak up in the first place. The CHRGM *Gender-based Violence Disclosure Toolkit: Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings* offers detailed consideration about how to respect confidentiality of disclosure and support a survivor through the referral pathway.[35] With respect to referral practice in the context of remote service provision specifically, the following guidance from the GBV AoR offers these additional considerations: [36]

- If you are giving specific information to the survivor related to how to access services etc. ensure that she has a pen and paper if necessary, and that it is safe for her to write information down. Be aware of potential literacy issues when giving out information.
- If you are unsure of information, tell the survivor you need to check the information and can call them back (if safe to do so) or they can call you back.
- In the context of a general emergency or public health crisis in which mobility and operations are suspended or otherwise affected, it can be useful to know the following:
    - Which current referrals pathway partners (e.g. service providers already identified in the existing referral pathway) continue to be open for services? Are referral pathways up to date?

- How will caseworkers work with referral partners? How will referral partners communicate to caseworkers about any changes to their services, including contact information, etc.?
- If phone-based case management services are able to take new clients from referral partners, how will referral partners share information with prospective clients about the remote case management services? How will referral partners share information with caseworkers/supervisors about new referrals?
- Is it possible or appropriate for those service providers that are remaining open and have appropriate transmission precautions in place (e.g. healthcare providers) to have phones and private calling spaces available where clients can call their caseworker? If so, are staff available to clean these spaces and equipment after each call?

Staff training and care

General staff training on GBV is critical to supporting safe GBV disclosure. In fact, CHRGM guidance recommends an all-of-team approach, since it is impossible to know which staff members might receive a disclosure of GBV. It may be anyone from the psychologist to the security guard, from the receptionist to the shelter cook.[37] There are of course specific skills and competencies a staff must have in order to prepare for and respond appropriately to GBV disclosure in remote service provision contexts. The GBV AoR's *COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines* contains extensive guidance for ensuring that an organization's staff receives the training it needs when pivoting to phone-based operations[38] (though many of these points are also relevant for video-conferencing):

- Operation of relevant apps to provide remote services (e.g. WhatsApp);
- How providing support via phone is different than in person, and what basic adaptations need to be made;
- Essential phone manners, e.g. initial greeting, speaking clearly and slowly, not speaking over the client, etc;
- Phone listening skills, e.g. active listening and listening for changes in tone without body language; use of silence; building trust and rapport on hotline;
- Standard call-handling protocols in line with basic case management steps (e.g. introduction, assessment, case and safety planning, referrals, call closure);
- Managing a call with a minor;
- Managing calls when clients are at immediate risk and/or when a call is picked up by a perpetrator;
- Managing calls when clients are distressed or suicidal;
- Review of updated referral pathways and providing referrals over the phone;
- New data collection and management responsibilities.

It should also be noted that receiving GBV disclosure in remote service provision settings can be uniquely stressful or upsetting to practitioners. While research on impacts of remote service provision on practitioners is limited at this time, it is not difficult to imagine the ways constantly preparing for and responding to GBV disclosure at distance can affect providers. For example, constantly scanning for non-verbal or visual cues or possible retraumatization over phone or video-conferencing platform can be mentally and emotionally exhausting. Being unable to physically comfort a survivor by offering tissues or lightly touching their hand may contribute to providers' feelings of helplessness or ineffectiveness. Having a caller hang up suddenly can cause stress for the person trying to help them safely. It is critical for the care of a service providing team, and the quality and longevity of their individual work, to understand and mitigate the impacts remote work can have on practitioners who interact with GBV survivors.

Endnotes

[1] This guidance note is issued in conjunction with 2020-2021 multi-country study, *Choosing to Speak, Learning to Hear: Disclosure of Gender-Based Violence in Humanitarian Crisis Settings*, and practitioners' toolkit, *Gender-based Violence Disclosure Toolkit Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings*, both produced by the Center for Human Rights, Gender and Migration at Washington University's Institute for Public Health. These resources can be found in multiple languages at: https://publichealth.wustl.edu/centers/chrgm/chrgm-projects/gbv-disclosure-project/.
[2] UNICEF, "Innovative Approaches to GBV Service Provision in Emergencies". https://www.unicef.org/media/83381/file/Innovative-GBV-Service-Provision-Emergencies%20.pdf#:~:text=Safe%20spaces%20for%20women%20and%20girls%20have%20been,content%20for%20women%20and%20girls%20beyond%20SRH%20information.
[3] IRC, International Rescue Committee, "Guidelines for Mobile and Remote Gender-Based Violence (GBV) Service Delivery", 2018. https://gbvresponders.org/wp-content/uploads/2018/10/GBV-Mobile-and-Remote-Service-Delivery-Guidelines_-final.pdf.
[4] IASC Reference Group on Mental Health and Psychosocial Support, "Guidance: Operational Considerations for Multisectoral Mental Health and Psychological Support Programmes during the COVID-19 Pandemic", *Inter-Agency Standing Committee*, 2020. https://interagencystandingcommittee.org/system/files/2020-06/IASC%20Guidance%20on%20Operational%20considerations%20for%20Multisectoral%20MHPSS%20Programmes%20during%20the%20COVID-19%20Pandemic.pdf
[5] Dorcas Erskine, "Not just hotlines and mobile phones: GBV Service provision during COVID-19", *UNICEF*. https://www.unicef.org/media/68086/file/GBV%20Service%20Provision%20During%20COVID-19.pdf
[6] The GBV AoR is part of the InterAgency Standing Committee cluster system, working to prevent and respond to GBV in emergencies around the world.
[7] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-based Case Management and hotlines", 2021, https://gbvaor.net/sites/default/files/2021-01/covid-guidance-on-remote-gbv-services-04012021.pdf.
[8] NNEDV, The National Network to End Domestic Violence, "Digital Services Toolkit", Technology Safety. https://www.techsafety.org/digital-services-toolkit
[9] NNEDV, "Digital Services Toolkit".
[10] NNEDV, The National Network to End Domestic Violence, "Step By Step Guide," Technology Safety, https://www.techsafety.org/step-by-step-guide.
[11] Michelle Webb et al., "Best Practices for Using Telehealth in Hospice and Palliative Care," *Journal of Hospice & Palliative Nursing* 23, no. 3 (June 2021): 277–85, https://doi.org/10.1097/NJH.0000000000000753.
[12] PAHO, Pan American Health Organization, "Remote Delivery of MHPSS (Mental Health and Psychosocial) Interventions," September 2020, https://www.paho.org/en/documents/remote-delivery-mhpss-mental-health-and-psychosocial-interventions.
[13] Robert M Bilder et al., "Inter Organizational Practice Committee Recommendations/Guidance for Teleneuropsychology in Response to the COVID-19 Pandemic," *Archives of Clinical Neuropsychology* 35, no. 6 (August 28, 2020): 647–59, https://doi.org/10.1093/arclin/acaa046.
[14] PAHO "Remote Delivery of MHPSS (Mental Health and Psychosocial) Interventions."
[15] NNEDV, National Network to End Domestic Violence, "Video Conferencing & Digital Communication Platforms: Comparison Chart" (2020), at 1. https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5e7e62a25ed80a4219adad77/1585341091261/NNEDV_Communication+Tools_Handout.pdf.
[16] GSMA, "The Mobile Gender Gap Report 2022", June 2022. https://www.gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-Gap-Report-2022.pdf?utm_source=website&utm_medium=download-button&utm_campaign=gender-gap-2022.
[17] IRC, International Rescue Committee, "The Essentials for Responding to Violence Against Women and Girls During and After COVID-19," June 2020, https://www.rescue.org/report/essentials-responding-violence-against-women-and-girls-during-and-after-covid-19.

[18] GBV AoR, "Harnessing Technology to Prevent, Mitigate and Respond to Gender-Based Violence in Emergencies," November 2019, 26.
[19] With minor modification, these considerations are drawn from GBV AoR Helpdesk *et al*, *COVID-19 Guidance on Remote GBV Services Focusing on Phone-based Case Management and Hotlines* (2021), with specific reference to pages 6 and 12.
[20] NNEDV, "Video Conferencing & Digital Communication Platforms: Comparison Chart" (2020), at 6-7.
[21] For in-depth guidance, see National Network to End Domestic Violence (NNEDV), *Safety Net Project*, *Best Practice Principles for Digital Services*. Available at: https://www.techsafety.org/best-practice-principles.
[22] For in-depth guidance, see National Network to End Domestic Violence (NNEDV), *Safety Net Project*, *Using Zoom: Safety, Privacy, and Confidentiality Considerations*. Available at: https://www.techsafety.org/using-zoom.
[23] Adapted from National Network to End Domestic Violence (NNEDV), *Safety Net Project. Communicating with Survivors Using Video: Best Practices* (2020). Available at: https://www.techsafety.org/video-best-practices.
[24] Platform descriptions current as of 2019. Taken from conference paper, J. Botha, C. van 't Wout, L. Leenen. (2019). "A Comparison of Chat Applications in Terms of Security and Privacy. Available at: https://www.researchgate.net/publication/334537058_A_Comparison_of_Chat_Applications_in_Terms_of_Security_and_Privacy
[25] These tips are drawn from NNEDV, National Network to End Domestic Violence, Technology Safety, "Best Practices for Mobile Computing Devices," Technology Safety, available at https://www.techsafety.org/resources-agencyuse/mobilecomputing-bestpractices and National Democratic Institute, *Gender Women Democracy*, "COVID-19 Related Guidance How to Conduct Violence Against Women Programming Using online or Distance Engagement Methods," June 2020, available at: https://www.ndi.org/sites/default/files/ACFrOgBJS7xYrQaaB6vaJ0V7K5UVGnJPAeEU19Fae7kA11dtZxaWIPcNQ0sZ5HLKj5kFDdt_BrgqbTF0mPpRiV9nrZXHy845tzwJ283MytktmTjFluRALgWNsIXF-VKPZ7fs5QVipY76jM4wUuTp.pdf.
[26] CHRGM, Center for Human Rights, Gender and Migration, "Gender-based Violence Disclosure Toolkit: Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings," September 2022. https://publichealth.wustl.edu/items/gbv-disclosure-toolkit/
[27] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines."
[28] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines."
[29] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines," and International Rescue Committee, "The Essentials for Responding to Violence Against Women and Girls During and After COVID-19."
[30] Canadian Women's Foundation, "Signal for Help". https://canadianwomen.org/signal-for-help/
[31] CHRGM, Center for Human Rights, Gender and Migration, "Choosing to Speak, Learning to Hear: Disclosure of Gender-Based Violence in Humanitarian Crisis Settings," September 2022. https://publichealth.wustl.edu/items/choosing-to-speak-learning-to-hear/
[32] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines."
[33] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines," 35.
[34] These pointers are drawn from GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines," 34. See also Bilder *et al*., "Inter Organizational Practice Committee Recommendations/Guidance for Teleneuropsychology in Response to the COVID-19 Pandemic."
[35] CHRGM, "Gender-based Violence Disclosure Toolkit Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings," Module 1, Tool 4.
[36] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines," 13, 34.
[37] CHRGM, "Gender-based Violence Disclosure Toolkit Responding to Gender-based Violence Disclosure in Humanitarian Crisis Settings," Module 1.
[38] GBV AoR, "COVID-19 Guidance on Remote GBV Services Focusing on Phone-Based Case Management and Hotlines," 17.

Acknowledgments

This guidance note was drafted by Kim Thuy Seelinger, CHRGM Director and Associate Professor of Social Work, Public Health and Social Policy at Washington University. She served as Principal Investigator for this overall project. It was designed by Adriana Aramburu-Graypel, CHRGM Center Manager. The CHRGM team is grateful to Nikia Crollard for underlying research and Julia Uyttewaal for early support.

The study and project outputs were funded by the United States Government (Department of State, Bureau of Population, Refugees and Migration (BPRM)), with supplemental support from an anonymous donor to the Center for Human Rights, Gender and Migration.

Annex

ANNEX 1: Comparison chart of video-conferencing platforms (2020)

Platform	Functions	Access considerations	Privacy / Security Considerations
Zoom	Online video for one-to-one or groups Includes text chat function; Allows for recording.	Strong on accessibility for Deaf users; allows for closed captioning & American Sign Language interpretation; New users are asked to download the app and supply an email address, which may create technology and safety barriers.	Chat within video is end-to-end encrypted, but not video itself without additional agreement; Not most private by default, requires an additional agreement between agency and Zoom for higher level of security.
Gruveo	Online video for one-to-one or groups.	No closed captioning or separate option for ASL interpretation; but ASL interpreter can be a member of a group video chat; Quick access by clicking a link; no download or user information required.	End-to-end encrypted; strong on privacy, as of 2020.
Cyph	One-to-one chat, video, or voice. Group chat & group video pending as of 2020.	No closed captioning or separate option for ASL interpretation as of 2020; Quick access by clicking a link; no download or user information required.	End-to-end encrypted; strong on privacy, as of 2020.
Doxy.me	Online video for one-on-one communication	No download necessary.	End-to-end encryption, to ensure that personally identifying information (PII) is not stored or shared by them agency must sign additional agreement.
Resource Connect	One-to-one text or chat through a managed portal; group chat coming soon; internal group chat. Routing of hotline calls.	Multiple languages and alphabets supported (not including translation).	End-to-end encryption and no-knowledge platform, strong on privacy based on current practices.

This comparison chart was compiled in 2020 by the National Network to End Domestic Violence. It is available at: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5e7e62a25ed80a4219adad77/1585341091261/NNEDV_Communication+Tools_Handout.pdf.

Center for Human Rights, Gender and Migration

INSTITUTE FOR PUBLIC HEALTH AT WASHINGTON UNIVERSITY