Going Online

EPIC PROJECT

MAY 2024

Strengthening the Security of Virtual Client Support

A GUIDE FOR KEY POPULATION HIV PROGRAMS PROVIDING VIRTUAL CLIENT SUPPORT IN HOSTILE SETTINGS

PEPFAR

USAID FROM THE AMERICAN PEOPLE

EpiC Meeting Targets and Maintaining Epidemic Control

Table of Contents

Acknowledgments

This guide was written by Benjamin Eveslage, Katie Conner, and Abrahim Simmonds, with additional contributions by Robyn Dayton and Maggie McCarten-Gibbs. We are grateful to reviewers Hally Mahler and Michele Lanham. It was edited by Sarah Muthler.

Suggested citation: EpiC. Strengthening the Security of Virtual Client Support. Version 1. Durham (NC): FHI 360; 2024.

Photo credits

Page 6 photo by Anubhav Shekhar (Unsplash)
Page 10 photo by Emmanuel Ikwuegbu (Unsplash)
Page 13 photo by Fame of God Studios (Unsplash)
Page 17 (box 2) photo by Stefano Pollio (Unsplash)
Page 19 (box 3) photo by Adrian Swancar (Unsplash)
Page 22 photo by Olumide Bamgbelu (Unsplash)
Page 24 photo by Francisco Venancio (Unsplash)

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID) and the U.S. President's Emergency Plan for AIDS Relief (PEPFAR). The contents are the responsibility of the EpiC project and do not necessarily reflect the views of USAID, PEPFAR, or the United States Government. EpiC is a global cooperative agreement (7200AA19CA00002) led by FHI 360 with core partners Right to Care, Palladium International, and Population Services International (PSI).

Background

This guide was developed for key population (KP) HIV programs to secure their implementation of virtual support and referral of clients to HIV services in hostile settings.

Purpose

KP HIV programs should review and adapt this guide to their local and population context and then deploy it through trainings with staff who provide virtual client support, such as peer educators, online outreach workers, and peer navigators/case managers.

This guide is designed to mitigate security risks to both program implementers and clients that may occur as a result of virtual client support via (1) work devices and apps, (2) virtual communications with clients, and (3) processes for referring clients to in-person services. It includes program level guidance for use by managers, designers, or leaders of KP HIV programs during the design of programs and activities, as well as guidelines designed to be used by virtual client support staff. Several helpful tools for rolling out this guidance and adapting general telehealth approaches are included in the annexes. For additional strategies to mitigate risks from implementers' personal devices and communications, other staff cadres, other program activities, or broader organizational reputation and exposure, consider complementing this guide with related safety and security resources listed in Annex 6. Additional Resources.

This resource is designed for use in hostile settings where risks are posed by individuals who wish to do harm to key populations or KP program implementers using conventional approaches such as trolling, doxing, cyberstalking, cyberbullying, and particularly catfishing. In hostile settings where risks are posed by individuals or entities capable of sophisticated cyberattacks such as hack of data systems or devices, the approaches in this guide can reduce risks but are not sufficient to adequately address sophisticated attacks.

KEY TERMS

Hostile settings: Places with high social stigma and/or laws criminalizing specific populations, where harm is directed to these populations, and where human rights violators may be met with impunity

Virtual HIV interventions: Use of telecommunications platforms to remotely reach and engage clients in HIV services

Trolling: Sharing unwelcomed content within an online conversation to purposefully instigate an argument with one or more people

Doxing: The act of publicly providing personally identifiable information about an individual, usually via the internet, without their consent, and with malicious intent

Cyberstalking: Use of the internet and other technologies to harass or stalk another person online, including behaviors that intend to intimidate victims or make their lives unbearable

Cyberbullying: Use of technology to harass, threaten, embarrass, or target another person

Catfishing: The creation of a fictitious online persona or fake identity (typically on social networking platforms), with the intent of deception, usually to mislead a victim into an online romantic relationship or to commit financial fraud

Entrapment: Tricking someone into committing a crime to secure their prosecution, such as a police officer catfishing a suspected member of the LGBTQ community to get evidence to arrest them

Digital security risks and the functions available on mobile devices and virtual platforms and tools continue to evolve rapidly, as do legal frameworks governing both virtual spaces and threats to those spaces, and legal frameworks more broadly. While the contents of this guide and recommended processes should be relevant in the future, programs should continuously monitor developments, new risks, and legal changes, and adapt their plans accordingly. Programs should also consider the potential for future negative policy developments, such as the criminalization of activities not currently illegal, and the fact that information put online today cannot be retracted later should it become a liability. The Going Online team at FHI 360 can be reached for additional assistance at GoingOnline@fhi360.org

Context

Hostile settings are characterized by high levels of social stigma against and/or laws criminalizing KP, and impunity in the face of human rights violations. KP-focused HIV programs in hostile settings are commonly afflicted by myriad security concerns, including verbal, physical, and sexual violence toward staff; damage to organizational reputation and registration status; theft and property damage; and arrests of program participants, implementing staff, and civil society organization (CSO) management during or because of participation in program events.

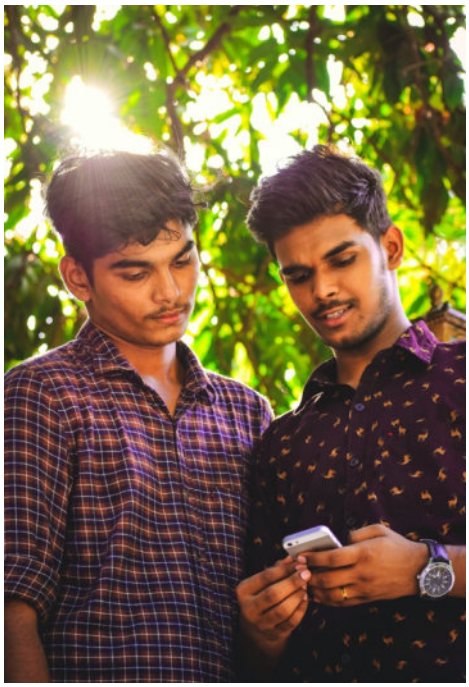
Virtual channels enable KP HIV programs to implement outreach and education with clients remotely and at a safer physical distance. For instance, physical violence, arrests, and some forms of discrimination can only occur in person. Providing support to clients virtually can mitigate these risks. Virtual platforms can protect both program implementers and clients because communication can be transmitted remotely, and users may use pseudonyms, anonymous profile images, and secondary phone numbers, offering more privacy.

However, virtual channels and devices also present novel security risks for KP HIV programs to consider and mitigate. Virtual channels conceal the identity and motivations of people who intend harm against program implementers and clients. Risks in the virtual space include trolling, doxing, cyberstalking, cyberbullying, and catfishing – each of which can result in physical, emotional, social, and economic harm to program implementers and clients. These risks are of particular concern where the virtual identity of program implementers and clients can be linked back to their physical identity, family, workplace, and social network.

Devices that enable virtual client support, such as mobile phones, tablets, and laptops, also present security risks. Unsecured devices can make it easier for sensitive information to be exposed or accessed by individuals who may use such information to identify and harm program implementers or clients.

Preparation

Practical steps to prepare for implementing secure virtual client support



The guidance below outlines practical steps that can be taken by managers, designers, and leaders of KP HIV programs, as well as virtual client support staff, to prepare for secure implementation of virtual HIV support and service for key populations in hostile settings. Implementers and service providers should review these recommendations and consider adaptations to fit their own program and population contexts.

Below are several important tasks for program staff to consider while preparing for virtual client support. Please note that these tasks may not be exhaustive, particularly for broader telehealth approaches. For a high-level review of considerations for adapting a broader range of telehealth and virtual HIV interventions in hostile settings, see Annex 1. In hostile settings, some approaches may not be appropriate, while others will need to be tailored to the risks experienced by program implementers and clients. Most recommendations in this guide can be used to strengthen all KP HIV programs, however, those recommendations that may only be relevant or necessary for hostile settings are noted by an alert icon ⚠.

1. **Identify experts:** Determine who may contribute knowledge and resources for programs preparing for and implementing virtual HIV interventions in hostile settings, for instance, legal experts to support legal analysis, dating app focal points to coordinate on community security messaging, human rights lawyers or advocates who can assist with incidents of violence or arrests, and community representatives to provide input and insight into community fears, needs, and experiences. The FHI 360 Going Online team can offer expert technical assistance in using and adapting this guidance (email GoingOnline@fhi360.org).

2. ⚠ **Legal analysis:** Conduct legal analysis with support of an expert to identify legal and security risks for clients, providers, and programs planning to implement virtual HIV services. Regularly review the status of local laws and their implications for KPs and service delivery to ensure protocols are up to date on latest developments.[1]

[1] Types of laws and policies to review may include data protection and privacy laws, cybersecurity laws, laws/policies governing health services, and laws that can be used to criminalize your target audiences/clients and people who may interact with them. The legal analysis should address these questions: (1) What are the legal risks for clients, programs, CSOs, and service providers

3. ⚠ **Risk analysis:** If risk analysis has not occurred or the existing analysis focused only on physical security, ask about harm that implementers have experienced in a virtual space, their perceptions of pressing virtual security risks, and service delivery preferences that could best mitigate those risks. Various sources should be consulted, including service providers, program implementers, clients, and new online target audiences. Use an anonymous online survey and avoid branding or limiting the survey to only KP members.[2]

4. ⚠ **Establish security team** or enlist an existing team in virtual security efforts: Each organization should designate employees at all levels to form a security team. The team should designate a security coordinator/officer to manage all security needs in the field and to act as a focal point who shares information with others and collects information when harms occur. Depending on the extent of the virtual portfolio, it may be important to hire someone with a technology background for this role.[3]

5. ⚠ **Contingency planning:** If none exists or if the existing contingency plan focuses only on physical security concerns, develop a contingency plan that specifies possible severe security events for clients or programs (e.g., arrests, office or online data breach) and details steps to be taken if these security events occur. A contingency plan should include a clear process of communication, such as an emergency call tree triggered when an incident occurs. Additionally, the plan should include emergency response procedures during office hours, outside of office hours, and when staff are on leave or traveling.

6. **Develop/revise terms of reference** (TOR) or scope of work to define the role of staff who provide virtual client support, such as online outreach workers, peer educators, and case managers. The TOR should include position requirements, daily activities, expected outputs and outcomes, and a code of conduct with respect to ensuring client privacy/confidentiality (see annexes 3 and 4 for sample terms of reference and code of conduct). Programs should consider selecting existing peer educators who already have skills in social media and virtual client support or hiring new staff with these skills.

---

involved in HIV services for key populations? (2) What are the penalties for breaking these laws? (3) What adaptations should be made to the program design to avoid breaking laws? (4) What additional non-legal risks should be considered due to social stigma and lacking legal protections or enforcement of legal protections for programs, clients, and service providers?

[2] Items 3-5 above may be completed as part of a broader security assessment if risks related to virtual platforms are incorporated. Learn more about security assessments tools by reviewing the tools and content included in the training document "Strengthening the Security of HIV Service Implementers Working with Key Populations."

[3] Security team responsibilities: (1) Inform the focal point of threats, risks, consequences, and developments; (2) define strategies to regularly assess, prevent, mitigate, prepare for, respond to, and recover from risks and their negative consequences; (3) develop, maintain, and update safety and security policies, plans, and protocols; (4) ensure workers have the knowledge and capacity to implement safety and crisis responses, including access to tools and guidelines to support deployment; (5) ensure compliance with safe practices is maintained and adhered to throughout the organization; and (6) communicate important threat alerts and notifications to decision-makers and management on a regular basis, and liaise with agencies, partners, and other external groups.

7. **Procure and set up devices and mobile data** for outreach workers and other applicable staff to use for their online HIV outreach activities, including a SIM card with new phone number used for work activities. See more under device security.

8. **Consider and select a secure system** to manage and track the efforts of online HIV outreach workers. For instance, the Online Reservation and Case Management App (ORA) is a web app accessible to clients who have a smartphone to book their own appointments for services offered by the online outreach workers. ORA also can be used by online outreach workers to book appointments on behalf of clients for virtual consults for HIV prevention education, HIV testing, self-testing, and to make referrals to other providers for a range of services. The system has functions to assign all appointments to the right outreach worker. Consider whether the appointments booked on ORA should collect client KP status. It is possible to turn off this question on ORA's appointment booking form, and outreach workers instead can rely on their individual communication with clients to ensure all clients who are booked on ORA are part of the program's target audience. See more guidance on ORA here.

9. **Create a network of referral providers** including service providers that can serve the broader general population (⚠ important in hostile settings focusing on key populations to ensure the outreach staff can remain useful to the general population and avoid security risks of being framed as KP-focused).

10. **Develop/update standard consent language** and Terms of Use/Privacy Policy that can be used by online outreach workers, peer educators, and case managers as they interact with clients. This policy should comply with local laws, funder agency requirements, and relevant local partner policies. The policy should be written in clear language for the client to understand which data may be collected from them, and how it is used, processed, and stored securely. A short consent question should be drafted that allows the client to understand and consent to the policy before any data are collected from them (see a sample Client Terms of Use policy for ORA in the annex and consent question in the communication guidance section).

11. **Develop training materials** for virtual client support staff, which may include a training based on an adapted version of this guidance as well as additional topics not covered in this guide. See Annex 2 for a sample training agenda. Standard operating procedures should be provided to each online outreach worker, specifying the step-by-step instructions for completing each of their routine activities.

12. **Review and ensure your compliance with the community guidelines** or other terms of service policies of apps used to communicate with clients to avoid being blocked by users or banned. For instance, see the WhatsApp Terms of Service and Grindr Community Guidelines.

13. **Create and maintain a work schedule for virtual client support staff**, including by reserving specific hours to (1) offer clients' appointments for virtual consults (appointment availability can be specified on ORA or in a calendar), (2) conduct routine outreach and messaging with clients, (3) follow up clients to reschedule missed appointments or other needs, and (4) complete other

activities like team meetings and reporting. The TOR and work schedule may determine whether virtual client support staff should only use work devices and conduct work activities from secure offices, or are permitted to use them in secure personal environments.

14. **Set up an online referral system** such as ORA for designated virtual client support staff to manage online appointment booking and follow-up to clients. This will include adding user accounts for virtual client support staff, adding service providers, services offered, and hours of operation, as well as customizing settings for the program (i.e., front-end language, SMS message content). FHI 360 can provide technical assistance for the set-up and customization of ORA.

15. **Create or revise profiles for outreach workers** on WhatsApp and other platforms that will be used to communicate with clients. See more under "creating/updating profiles."

16. **Train virtual client support staff**: Schedule a training with all virtual client support staff and supervisors using the developed training materials, adapted SOPs, and sample practical activities to simulate each step of client interaction. During the training, complete exercises where client support staff must identify security risks and describe how they would respond to them (e.g., What would you do if a client threatened to blackmail another client support staff member? What would you do if your device were stolen?). Make sure that their answers align with the protocol that you have set forth and trained them on. See Annex 2 for a sample training agenda. Prior to training, ensure all preparation tasks are completed. Upon completing the training, staff implementing virtual client support should agree to and sign a confidentiality statement or code of conduct (see sample in Annex 4). After the training, virtual client support staff should have easy access to their secure work device, secure internet access, SOPs, TOR, code of conduct, and terms of use policy/data security policy.

17. **Scale up iteratively**: Under close supervision, virtual client support staff can begin using their secure work devices and applying their new guidance to their routine client support activities. Supervisors should closely monitor the steps staff take when interacting with new clients and referring them to services to ensure they are following the SOPs and not endangering clients, themselves, or the organization. For new cadres of staff, such as specialized online outreach workers, start by implementing the approach with a few online outreach workers who can follow the communication guidance to reach out to existing clients, provide support, ask for referrals. The outreach team should review lessons and troubleshoot with their supervisor any challenges or risks they encounter, which may require iterative adaptations to messaging and communication guidance. When working in hostile environments, supervisors should ask about security concerns during each supervision session. Expand rollout to the full cadre of online outreach workers and expand their outreach to new audiences gradually. Schedule routine weekly meetings with outreach workers, their supervisors, and other program staff to review results, optimize, name security challenges encountered, and address concerns. Also establish a secure WhatsApp or Signal internal group chat for the program staff and outreach workers so that immediate concerns and questions can be addressed outside meetings. Ensure that personally identifiable information of clients is not shared in messages or screenshots in the internal group chat.

Device and app security

Recommendations for program managers and virtual client support staff to use mobile devices and apps more securely

This section presents key considerations for setting up, securing, and managing devices used by virtual client support staff, particularly mobile devices like tablets and smartphones. See related guidance in FHI 360's Mobile Device Guidance or on the SafeQueers website.

Device security

1. **Use a mobile device management (MDM)** platform or functions to keep track of all devices and remotely manage devices. Program managers should consider purchasing work devices from a vendor that offers these functions. For example, by registering Samsung devices under one Samsung account, your organization will be able to use Samsung's device management functionalities to locate devices that have been lost or stolen and ring, lock, or wipe devices remotely. For this to work, each device must be connected to the internet and have the "Find My Mobile" feature enabled in the device settings. For non-Samsung Android devices, similar functionalities might be available through Google's "Find My Device." As an alternative, consider third-party MDM platforms.[4]

2. **Install an antivirus on each device** as this helps to detect and remove malware that will compromise the privacy or security of the devices. Install an antivirus software such as Avast or Endpoint Security.

3. **Create an Excel document to track devices and users:** Program or IT managers should create and keep

[4] Platforms like Miradore and Jumpcloud are free for use with a certain number of devices and limited features. Upgrading to a premium subscription provides additional features and allows you to manage a larger number of devices. Alternatively, the trusted international not-for-profit group TechSoup offers discounts to registered not-for-profit organizations for Microsoft Endpoint Configuration Manager Device Client and Cisco Meraki Systems Manager. These options are ideal for larger organizations with a lot of devices to manage.

updated a password-protected Excel document to list all virtual client support staff and key details of their devices, including staff name, title, phone number, WhatsApp number, email, SIM details/lock pin, and other account details. This will allow the program to easily identify who is using each device and how to manage those devices remotely if they are lost, stolen, or accessed by hostile parties/individuals.

4. **Enable encryption** to protect data stored on the device, especially if it becomes lost or stolen. On mobile operating systems like Android and iOS, device encryption can be turned on through the security settings (see step-by-step guidance for Android and Apple devices). Ensure that the password created to decrypt devices is strong (see guidance below). Avoid storing sensitive client-specific information (such as photos, screenshots, videos, and audio files) on the device's files and folders. If you do store such information, place it in encrypted or password-protected folders/apps rather than leaving it unprotected in general storage areas accessible without a password. See step-by-step guidance for setting up protected folders on Android or Apple devices.

5. **Lock devices using a strong password** to protect devices and mobile apps used by virtual client support staff. Use passwords that combine numbers and letters of the alphabet, especially for apps and lock screens. This is safer than a pattern password or biometric password, such as FaceID or fingerprint, that a hostile individual may more easily force staff to provide to access the device.

    - Passwords should have at least eight characters including numbers, letters, and symbols. Avoid using simple dictionary words and details from personal information like your name and birthday when creating passwords.

    - Avoid using the same password across accounts or devices to prevent credential stuffing, where hackers use leaked log-in information to access other platforms.

    - If you want to keep track of all your passwords, get a free password manager. There are several options available on each device's app store; some examples are 1Password, LastPass, and Dashlane.

6. **Regularly update device operating software (OS):** Check that each device's operating system software is up to date. Updating software is the best way to ensure that patches, designed to address current malware and virus threats, are in use.

7. **Secure mobile devices during transit and outside the office**. Workers should use nondescript cases to obscure the type of device they are carrying and avoid using devices in public where onlookers might view sensitive content. All devices should be kept physically secure and never left unattended. If online outreach workers will work from a designated office, consider whether they should leave devices in a secure storage at the office before returning home (this implies that outreach workers can only support clients virtually when they are physically within the office and not after hours).

App and website security

1. **Download and use the most secure messaging apps.** A secure messenger service can keep your online conversations private from advertisers and governments. The top three secure messaging apps for 2024 include Signal, WhatsApp, and Telegram. Read more on their unique encryption and security features here.

2. **Enable encrypted messaging options** within apps like Signal, Telegram, or WhatsApp to protect chat data through encryption. End-to-end encryption is already enabled on Signal, Telegram, and WhatsApp as a default, however, in addition, you may need to manually enable encryption of messages saved in backup files. See instructions for WhatsApp, Telegram, Signal. Note that anyone with your WhatsApp phone number can see your status, regardless of whether they have messaged with you before. Your status is not encrypted.

3. **Turn on disappearing messages** or "self-destruct messages" on chats with clients, where this function is available. When this setting is applied, messages will be automatically deleted on both the staff and client phones after viewing by the recipient or after a set period has passed (e.g., 24 hours).

4. **You can set passwords to limit access to some apps**. See instructions for applying a screen lock to WhatsApp on Android and Apple iOS.

    - Do not save sensitive or identifiable information about yourself or clients on apps:

    - Do not save a client's surname or other sensitive information as part of their contact details on your phone. Save only their first name (or their preferred nickname). Do not add compromising words such as "gay," "MSM," "Grindr," or "FSW" to client contact information as this could make them a target for harassment if data are accessed by unauthorized persons.

    - Follow additional guidance in the section on communication for how you agree on and communicate these preferences with clients.

5. Do not save photos, addresses, banking information, or personal notes that can identify you or a client on your device or chats. If personal client details are shared with you in a chat, record that detail offline or in your secure online client tracker tool (e.g., ORA) and delete it from the chat. Advise the client that you have done so. Even if chats are set to expire and delete within a certain time frame, it remains crucial to manually remove sensitive information as an added layer of security.

6. **Use two-factor authentication** on apps and websites, where available. Two-factor authentication (2FA) provides an extra layer of security beyond a password for logging into apps, websites, and online accounts. It works by requiring two types of credentials for login:

    - A password or PIN that you should already know (Follow guidance for creating strong passwords)

- Then, an authentication code that is generated from an app or sent as a text message.

7. **Always log out fully** of web and mobile app sessions when work is finished, especially on shared devices. Do not just close the app.

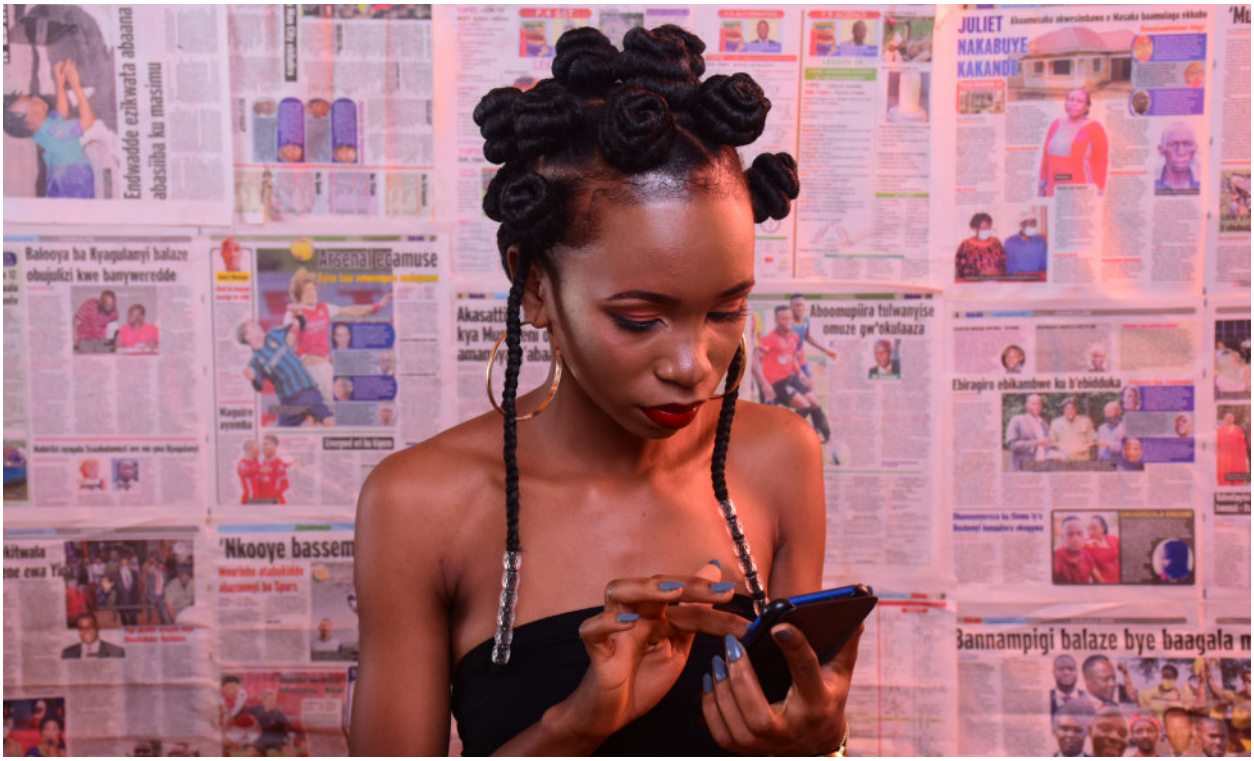
8. **Rename shortcuts or decoy home screen icons** of sensitive apps. For example, on apps like Grindr, you may use an icon such as a calculator to decoy the app, in the event the device becomes lost, stolen, or compromised. Use device features like Secure Folders on Samsung Knox to add a second layer of password protection.

Connecting to the internet securely

1. Always connect your work devices to the internet on a secure connection, for instance office Wi-Fi network or mobile data connection (from a work-procured SIM card).

2. Avoid connecting to the internet by other means, such as public Wi-Fi, internet café, or a friend's mobile hot spot that may be used to monitor your online activity. Public spaces also do not provide a private or confidential environment to communicate with clients.

3. If you use an insecure internet connection, use a virtual private network (VPN), which allows you to connect to the internet anonymously and helps you get around blocks and access censored sites. Learn more about how to set up and use a VPN.



Virtual communications

Recommendations for virtual client support staff to create profiles and communicate with clients securely

Creating/updating profiles

1. **Create new profiles** for virtual client support staff on secure messaging apps like WhatsApp, Signal or Telegram, by registering their new work phone number procured by the project. The WhatsApp Business App[5] is recommended, or similar business profiles on other apps, if available.

2. **Add profile details, based on program guidance:** In less hostile settings, virtual client support staff may be more open about the organization they work for, show their real name, and use a professional photo on their profile. However, if there are concerns about blackmail — for example, if the virtual client support staff are not open with their family, school, or job about their KP status — using non-identifying information is safer. ⚠ For hostile settings consider these recommendations:

    - **Name:** Use a nickname rather than a real name. Choose a professional, anonymous nickname to use and present on your profile and every time you communicate with clients. A nickname can be selected at random but should be professional; for instance, an outreach worker with legal name Benjamin can use "Jonny" as his nickname, and he should always call himself "Jonny" in in-person and online communications with clients.

    - **Profile photo:** Create or choose a professional avatar or profile image that conceals the identity of the staff (which can be created within WhatsApp easily). Additionally, do not send images of yourself to clients during routine chats.

    - **Bio text:** Use a broad bio text that is not specific to key populations or HIV and avoids mentioning the organization or project name. "I am a community outreach worker providing free sexual health information and services to people in [Country]. Ask me a question!" See the virtual communication guidance for steps to build trust with clients and eventually share more specific information about the project and your services.

[5] Note: WhatsApp considers chats with businesses that use the WhatsApp Business app or manage and store customer messages themselves to be end-to-end encrypted. Once the message is received, it will be subject to the business's own privacy practices. The business may designate a number of employees, or even other vendors, to process and respond to the message. Read more here.

Virtual communication guidance

This section provides guidance for outreach workers to conduct routine individual online outreach and virtual consultations.

STEP 1: REACH OUT TO EXISTING CLIENTS

Reach out to existing clients on WhatsApp that you know and trust on your new work profile. Reintroduce yourself with your new nickname and tailor the messaging script below to assist these clients through the process of identifying their service needs and supporting them to access services. Also support clients to turn on chat lock and disappearing messages.

> ***"Hey! I am going to send you a message on my new work profile under the name 'Jonny'"***

Send the above message from the previous account you used to communicate with the client.

> ***"Hey! How are you? I am contacting you on my new work profile. I am using my new nickname 'Jonny.' As always, I am available here to address your questions about health services and information."***

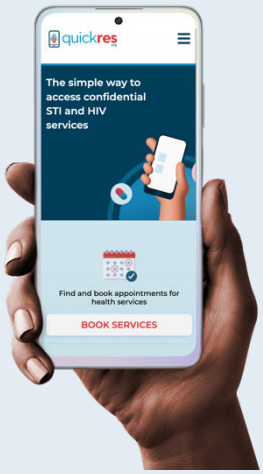
> ***"To protect your privacy, I recommend saving my contact in your phone as 'Jonny helper' or something discreet. Then select my profile and turn on 'chat lock' and then turn on 'disappearing messages after 24 hours.' Do you need any help applying these settings?***

See links above for step-by-step instructions to apply these security settings

For existing trusted clients, you can proceed to the next step to ask for referrals and skip to steps 7-9 to book and host virtual consults with them or refer them for in-person services.

STEP 2: ASK FOR REFERRALS

Ask your trusted clients if they can refer other friends to access support and services from you. You can let the client make the introduction, or you can ask the client to share the contact information for the referred client for you to initiate outreach to them. Also ask if they are a member of any WhatsApp groups where you can find additional clients and discreetly share information about your services.



BOX 1. VIRUTAL COMMUNICATION FLOW

The virtual communication guidance spans 11 steps to ensure effective outreach, enrollment, and referral to in-person services, including:

1. Reach out to existing clients
2. Ask for referrals
3. Join group chats with caution
4. Build trust with new clients
5. Ask for client consent
6. Collect client details
7. Book virtual consult appointment
8. Prepare for upcoming virtual consults
9. Host virtual consult
10. Complete reporting
11. Additional follow-up actions

View a sample client conversation on YouTube to see these steps in action.

"I am happy I was able to help you! Do you have any friends who might also benefit from my support?"

"If you think referring this friend to me might put you, or your friend, at risk of harm, then let's skip referring that friend and consider someone else."

"To introduce your friend to me, send your friend a message like this: *'Hey! How are you? I received confidential health information and services from a friendly outreach worker named Jonny. Can I send you his contact information?'"*

"If you want me to contact your friend directly, should I mention that you referred them, or do I keep your identity anonymous?" I can send a message like this…"

Standard message: ***"Hey there, how are you? Your friend [name] recommended I contact you. My name is Jonny and I work at [local partner name]. I am available here to confidentially address your questions about health services and information."***

Anonymous message: ***"Hey there, how are you? My name is Jonny. I am available here to confidentially address your questions about health services and information."***

"Do you know of any WhatsApp group chats, or other groups, with people who can benefit from my support?"

"For each group, do you want to add me to the group, or do you want to send me the group admin's contact information so I can contact them directly?"

STEP 3: JOIN GROUP CHATS WITH CAUTION

Message the group administrator to introduce yourself, ask them about the purpose of the group, and ask their permission to share health information and interact with individual group members to support their access to health services. Never send a group message that specifically mentions an individual's HIV or population status, and keep group messages broad and inclusive. Group messages should invite members to start a private chat with you to discuss more. If you think the content of a group message may put you or other members at risk, review these concerns with your supervisor to consider if you should remove yourself from the group.

STEP 4: BUILD TRUST WITH NEW CLIENTS

Build trust with new clients by taking them through a series of steps to introduce them to the program, the services you provide, and to confirm they are a member of the target audience.

1. **Introduce yourself:**

   "Hey there! How are you? My name is Jonny. I am available here to address your questions about health services and information."

   From referral: ***"Your friend David said I could drop you a line, just to let you know I am here to help."***

From group: ***"I work for a community nonprofit in [city] and I help people access free health services. I saw you on [name of group] and wanted to reach out."***

Note: You can add more detail to your introductory message as relevant, for instance, how you found their contact information, and you can mention your title. However, in your introductory messages, keep the health and population focus broad.

2. **Secure the chat:**

   "We might discuss your personal health matters here, and I want to protect your privacy. I recommend saving my contact in your phone as 'Jonny helper' or something discreet. Reach out to me whenever you want."

   "For added security, can I turn on disappearing messages? Then, any messages sent here will auto-delete after 24 hours."

   "And if you like, you can also add a passcode to open this chat on your own, select my profile, and turn on 'chat lock.' Do you need any help applying these settings?"
   (See links above for step-by-step instructions to apply these security settings)

3. **Ask clients about their health needs:**

   "What kind of health information or services are you interested in?"

   If the client responds with health concerns outside the scope of the outreach worker, make referrals to other providers and let the client know they can reach back out for assistance. If the client shows interest in sexual health services offered by the outreach worker, proceed to the next step.

4. **Explain the sexual health information and services you can provide:**

   "I can help assess your sexual health needs, provide HIV testing, and make referrals so you can access many other sexual health services. Is there something you need now, or do you want to learn more about available services and see what is right for you?"

   Take note of the client's response and continue to the next step.

5. **Confirm client is a member of a target audience:** This is a very sensitive step and requires donor and organizational review to confirm the way questions are asked to clients do not put clients, outreach workers, or the organization at risk. Confirming this information may

BOX 2. CATFISHERS

Tips for identifying a catfish:

- Follow your instincts! ⚠
- Client is too insistent to meet in-person or asks for money, explicit content, or sensitive information. ⚠
- Blank profiles or profiles with inauthentic bio or images.
- Client has an inconsistent story or information.
- Profile was newly created and has few followers or friends on social media.

If you believe they are a catfish:

- ⚠ If you feel uncomfortable or the client is too insistent, stop all communication and consider blocking their profile. Report the person to your supervisor immediately.
- Do not provide them any sensitive information about yourself or your organization.
- If you can confirm they are a catfish and intending to do harm to you or others, report their profile.
- Discuss the case with your supervisor to decide how to handle it.

be done at this step, or the program can ask these questions during the initial virtual consult with the client, depending on the context. Consider the messages below and adapt based on context and need:

Broad message: ***"It's important for me to ensure I'm providing the right support. I offer specialized services for various groups who might face stigma. Please let me know if you're looking for this kind of support or if you're seeking general health services. You can reply with 'Yes, I am in the right place' or 'I want general health services.'"***

Specific message: ***"Before we start, let me explain that I provide stigma-free and confidential services, including for vulnerable populations. These can include women who offer sexual services, men who have sex with other men, transgender people, or related groups. You can reply with 'Yes, I am in the right place' or 'no, I want general population health services.'"***

For clients who respond, "Yes, I am in the right place," proceed to the next step.

For clients who respond, "I want general population health services," ask a bit more about what specific health services or information they are interested in, and respond to your ability and/or share referrals to local health providers.

Note: Some programs may decide to use a standard risk assessment/service navigation tools administered as questions asked via chat messenger instead of the single question above to determine if the client is a member of the target audience. Using this method may require more time from the outreach staff to administer these tools among a broader range of clients who may not be a member of the target audience.

STEP 5: ASK FOR CLIENT CONSENT

Use standard language that is clear for the client and aligns with national laws and organizational policies, and include a link to the organization's full Privacy Policy/Terms of Use.

"Do you consent for me to collect some information from you as part of my work, such as your nickname, date of birth, and phone number? I use this information to provide support to you and help you book appointments for services. You can find our full Terms of Use policy here: https://ORA.org/about"

For clients who respond affirmatively with "yes" or "agree," proceed to the next step. If the client does not agree, or they have additional questions or concerns, then address their concerns, and offer another opportunity for them to provide consent. For clients who do not consent, do not continue to subsequent steps. Instead, send a message like this…

"No worries! I understand your concern. Without your consent I will not collect any information from you, but I can still help you with sexual health questions and direct you to health providers."

STEP 6: COLLECT CLIENT DETAILS

Collect client details including by asking the client questions to generate their Unique Identifier Code (UIC) used by the project. In the WhatsApp chat, share with the client their nickname, UIC, date of birth, and phone number so you can easily use it later to book appointments for them. (When "disappearing messages" is turned on, these messages will be deleted after 24 hours). If this information is noted on a paper, shred or destroy the paper at the end of each day.

"To keep your identity safe, I'll create a unique code for you. May I ask a few questions to set this up? Your details will remain confidential."

Proceed to ask questions to generate UIC.

"Alright, I have your information saved as [nickname], UIC # [XXXXXXX], date of birth [DD/MM/YYYY], and phone number [##########]"

STEP 7: BOOK A VIRTUAL CONSULT APPOINTMENT

For hostile settings, it is important for the online outreach worker to first have an audio-only virtual consult with clients prior to any in-person meeting, video calls, or referrals. This is to protect the outreach worker and provide an opportunity to confirm the client is a member of the target audience and not likely to direct harm to them or their organization. Ask the client for their preferred time and book the appointment on ORA or on your calendar with their details above.

"To get started, can I schedule a virtual consult for us to discuss your specific sexual health needs? When are you available in a quiet and private location to receive a call from me?"

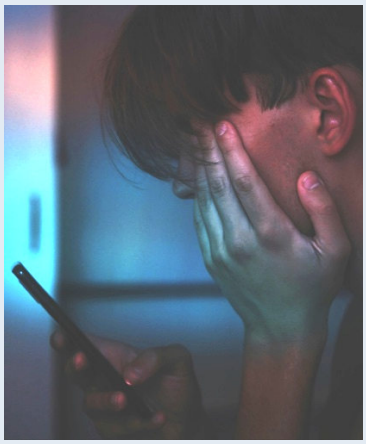
Let the client know when you are available for virtual consults based on your hours of availability and other consults already booked.

When using ORA: ***"When I book your appointment on ORA, it sends you text messages to remind you of the appointment. Will this be helpful, or should I turn off these text messages?"***

Book the appointment on ORA based on the client's inputs and communication preferences. Remind the client they may receive reminders by SMS, including instructions on how to connect for the consult 15 minutes prior to the call.

STEP 8: PREPARE FOR UPCOMING VIRTUAL CONSULTS

Prepare for your consults by logging in to ORA with your ID or checking your calendar, viewing appointments booked for today, and planning your tasks for the day. This can include preparing for virtual consults with clients, using your free time to reach additional clients online, responding to client chats, and performing other duties. ORA automatically sends clients an SMS appointment reminder 48 hours and two hours prior.



BOX 3. VIRTUAL HARRASSMENT & ABUSE

If you experience…

- Your personal or sensitive information was shared or published online.
- Threats of/actual blackmail
- Bullying or derogatory language
- Verbal threats of any type of violence
- Sharing of sexually explicit content or sexual advances
- Consistently pushing boundaries or violating stated purpose of the chat

Take the following steps…

- For a first-time mild offense, clarify your boundaries and the purpose of the chat. If you do not feel comfortable continuing to work with this client, refer them to another worker.
- For repeat offenders or clearly intentional violations, do not engage, cease communication, and block and report their profile.
- Report incidents to your supervisor and seek mental health services if you feel that would benefit you.

For virtual consults, another message is sent 15 minutes prior, with instructions for them to find a quiet and private place and prepare for your call.

Send the following message to the client a few minutes before their scheduled appointment:

> **"Just a reminder, your virtual consultation is scheduled soon. Please find a quiet and private space. Are you ready for our session?"**
>
> If the client requests to reschedule the consult, confirm the new time with them and edit the appointment record in ORA or your calendar accordingly.

STEP 9: HOST THE VIRTUAL CONSULT WITH THE CLIENT

At the date and time of the clients' scheduled appointment, follow the instructions below to start the call and cover essential elements. Conclude the call by booking additional appointments for the client on ORA or another platform for in-person or delivered services offered by the project.

1. **Call client** on the phone number shown on their record on ORA (tap the hidden phone number to reveal it) or contact them by the other contact information provided. This can be a standard voice call (free for the client) or a WhatsApp audio call. Avoid starting a video call with new clients.

2. **Introduce yourself discreetly.** Use your online nickname you shared previously, and do not yet mention your organization, health focus, or client name.

   "Hello, I am Jonny calling for your virtual consult. How are you?"

3. **Confirm the client's identity.** This is an important step to avoid starting the virtual consult with another person who may have picked up the client's phone and could pretend to be them.

   "Before we start, I just want to confirm I am speaking to the right person. Can I ask who I am speaking with?"

   "Great, thank you [client nickname]"

   "And can you confirm the date of birth you used when we booked this appointment?"

   If the client's responses above do not match the details on the appointment record on ORA, reply with a message like:

   "Sorry to bother you. It seems I have the wrong number. Thank you for your time and have a good day."

   Then send a message to the client on the secure WhatsApp thread like this:

   "I tried calling you on your number for our virtual consult today, but someone picked up who could not confirm your name or date of birth. Is there another time or phone number I should call so we can connect?"

4. **Outline the topics to be addressed** in the virtual consultation with the client. These include providing education on HIV prevention, arranging referrals for HIV self-testing (HIVST), HIV testing

services (HTS), antiretroviral therapy (ART), pre-exposure prophylaxis (PrEP), and post-violence support services. Additionally, the consultation can cover education on human rights. Explain that your organization offers a package of high-quality services that provide the client with holistic health assistance that works best as a whole. You can start with the service he asked for and then move on to the other services. Confirm if the client is okay with it. If not, try to persuade the client without being imposing.

5. **Continue to provide the "standard HIV prevention and education session"** to the client (based on existing organizational guides and materials). Explain that this session includes an assessment of the client's overall HIV education and service needs. This should take 30–45 minutes depending on their knowledge and topics they want to learn more about.

6. **Offer HIV screening or testing** to the client in the modalities offered by the organization. This may involve a separately booked future appointment for home-delivered HIV self-testing, an in-person meeting with the outreach worker to conduct a rapid HIV test, or an appointment at the organization office for testing. ⚠ For hostile settings, it is highly recommended that new clients first be directed to a health care facility and not be eligible for delivery or in-person settings for their first encounter.

7. **Refer clients for additional services**, including ART referral, PrEP referral, and family planning. Use ORA or any applicable platform to book appointments for services that are available within your organization, and direct clients to trusted providers for services not offered by your organization. You may prepare a referral slip and send a picture of it to the client if applicable or arrange for them to collect this slip in person.

8. **Feedback and client referral:** Offer the client the option to provide feedback on their virtual consult and refer friends for services on ORA, and conclude the virtual consult. You can explain this to clients with the following types of messages:

   "After our call, I will send you a link by SMS where you can complete a quick five-question survey to provide feedback on this virtual consult. If you have a smartphone with internet, you can submit the survey on your own, and I won't be able to see your feedback directly; it will be shared with my manager."

   "Lastly, do you have any friends you want to refer to me for a virtual consult?"

   If the client responds affirmatively, proceed to the next message. Otherwise, skip to concluding the consult.

   "I can send you a link where you can enter the phone number of each person you want to refer, and then ORA will send that phone number an SMS with instructions on how to book an appointment, or I can enter them for you now."

   "The messages sent by ORA to your referred friends are anonymous and do not reveal your identity. However, you can also call or message your friend to let them know you referred them – this is entirely up to you. After the referral is made on ORA, I only see their phone number so I can call or message them and invite them to schedule a virtual consult, but I will not reveal your identity."

   If the client has a smartphone with internet and wants to refer friends on their own, find their appointment on ORA, click "referral" > "client initiated" > "send link," then ORA will send them an SMS with link to access the client referral tool.

If the client requests your assistance to refer friends, click “referral” > “provider initiated” > “manage,” and then ORA will open the client referral tool on your device so you can guide the client through each question to complete one referral at a time.

Conclude the virtual consult with a message like this:

“Thank you for taking the time to meet with me today. Your next steps include: [mention all referrals and future appointments booked for the client, and any other follow up actions]. I will be in touch with you on WhatsApp, and you can always ask me questions on WhatsApp. Is there anything else I can help you with today before we close?”

Resolve any pending issues, then…

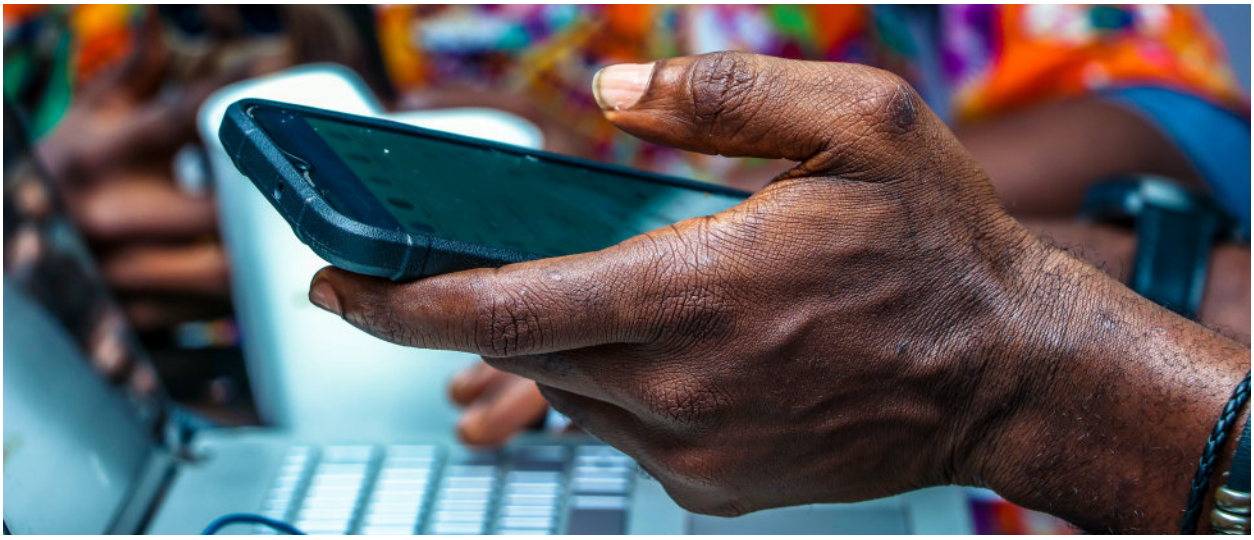
“Thank you and have a good day. We will be in touch! Bye!”

STEP 10: COMPLETE REPORTING ON ORA AND OTHER PROGRAM TRACKERS

On ORA, report that the client attended their virtual consult. Then, use standard program reporting tools (such as on a DHIS2 tracker) to report your interaction with the client, completion of the standard HIV prevention education session, referrals made, etc. (as required by the program).

STEP 11: ADDITIONAL FOLLOW-UP ACTIONS

Follow up on referrals made for the client to access additional services after the virtual consult, for instance, appointments booked for in-person services, requests for delivered services/commodities, and other types of virtual consults (e.g., mental health, human rights reporting, gender-based violence [GBV] support). Also, follow up on referrals made on the client referral tool on ORA, including by contacting referred clients, introducing them to the program, building trust with the client, and confirming their appointment details on ORA, whether for a virtual consult or HIV/STI screening/testing services, as relevant.



Referrals

Recommendations for virtual client support staff to refer new clients to in-person services.

The section below provides guidance for outreach staff referring new clients reached online/virtually to offline health services and support. For existing trusted clients, you can refer them to relevant CSOs for services.

Referring new clients to access services at CSO clinics/offices

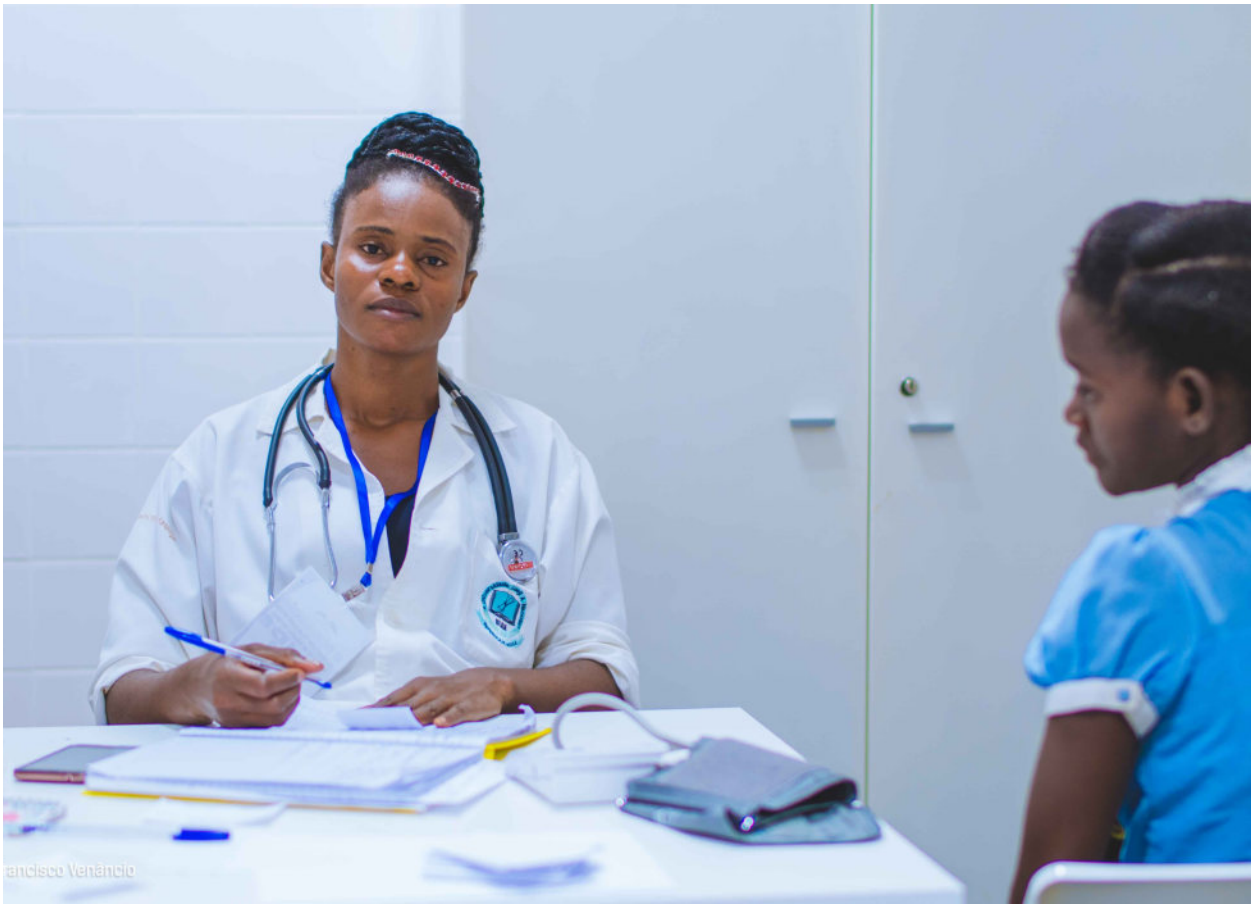
- If the client is referred by an established beneficiary, there may be more trust established with that referred client to link them directly to a relevant CSO for services.
- Do not refer any clients to CSO services if the outreach worker has not yet established trust with the client or if the client may be a catfish (see box 2) or was harassing or abusive to you or other program staff (see box 3).
- ⚠ In hostile settings, avoid referring new clients to KP-specific CSOs or drop-in centers (DICs) for their first service access (especially if the client was reached on social media, group chats, or other apps). For these clients, first follow the steps in the section above to conduct an audio-only virtual consult and refer them to a more secure service delivery modality (such as health care providers that are not primarily serving KPs but are known to the organization to be trusted entities or upcoming public outreach events in the community that are not KP-specific). After these new clients access services from those more secure service delivery modalities, the outreach worker may offer referrals to CSO services or an in-person meeting.

Meeting new clients in person

- ⚠ In hostile settings, it is not advised for an outreach worker to meet a new client in person for the first encounter. Start with an audio-only virtual consult to assess the client's intentions and service needs and to establish trust.
- It is not guaranteed that all in-person risks can be mitigated, but if the outreach worker and their organization deem it necessary to meet a new client in person, consider these security steps:
    - Select a public and more secure place to meet the client.
    - Inform the supervisor of the location and time of the scheduled in-person meeting. Sign in and out when going to the in-person meeting so that the supervisor knows you have returned. The supervisor may also track whereabouts by using GPS on the outreach worker's phone.
    - Ensure a coworker accompanies the outreach worker to the meeting to monitor the meet-up from a distance and can intervene or serve as a witness if a security situation arises.

- Arrive to the meeting place 20 minutes early to survey the surroundings and identify possible threats or traps.
- Do not identify yourself and your arrival until the client announces their presence and can be identified.
- Consult with your organization prior to meeting new clients in person to understand the protocol that you should follow in case of police arrest, raid, or other violence or harassment. The organization should share information on the financial, legal, medical, and mental health resources available to assist you in these situations so that you can make an informed decision about whether to take specific actions that might feel risky.

- Follow the steps listed above to secure your device and apps before going to the field to meet clients. If the device and apps cannot be secured completely or might be forced open by police or others, ask your organization to provide you with another secure device for use in field visits. Do not carry your own personal phone during the visit.



Supervision guidance

Strategies for guiding, supporting, and enhancing the performance of online outreach workers in virtual engagement and client management

Training

- Ensure all online outreach workers, peer educators, and other pertinent staff receive the full training, focusing on the creation of online profiles, engagement with clients in group and individual chats, use of ORA when applicable, security considerations, and support protocols should incidents occur, as outlined in your organization's guidelines and this guide.
- Provide training material and the SOP to online outreach workers and peer educators to consult during their routine activities.

Supervision and monitoring

- Oversee online outreach activities to ensure they align with the recommendations in this guide and your other program provisions. Regularly review the implementation of strategies and tactics to maintain high standards of service delivery.
- Conduct regular consultations with outreach staff to discuss their experiences, security incidents, perceived risks, and effective techniques in client support. Use these meetings for mutual learning, sharing new ideas, addressing challenges, providing support for well-being, and correcting deviations from established best practices, thereby enhancing the skills of staff and ensuring they feel supported. Additionally, these consultations can lead to updates in protocols based on the threat level and current climate.
- Assess online threats reported by staff and take appropriate action. If a particular social media platform or application is deemed a risk to the organization, tell staff to avoid accessing that site or group until further notice. Affected staff profiles may need to be deactivated following an incident, particularly if identifying information was revealed, and financial and legal resources provided to mitigate risk. If a serious threat is reported against the organization or staff, report the incident to the appropriate next level of command. It may be necessary to consult in-office security, hire additional external security, temporarily change locations, or close the office.
- Set and monitor performance indicators for outreach activities, such as client engagement rates, referral follow-ups, and successful service deliveries. Additionally, ORA can be used to generate cascade graphs for each worker, showcasing the number of consultations booked, appointments honored, and referrals for additional services. Analyze these trends to motivate and inspire the outreach team.
- Aid and support outreach workers facing technical challenges with virtual platforms, ensuring uninterrupted service delivery and client engagement.

- Develop protocols for managing crises and emotional distress encountered in online outreach. Be available to assist clients and staff in navigating difficult online situations. Collaboratively work with outreach workers to resolve conflicts or issues with clients and establish a system for disengaging from clients who pose threats to staff security.

Feedback and continuous improvement

- Actively solicit and incorporate feedback from outreach workers to refine strategies and tools. This process should aim to continuously improve client engagement and program effectiveness, and to mitigate risk.

- Review client feedback on ORA and other platforms to address adverse events and improve service quality. General review of client feedback should be conducted monthly, and supervisors should act immediately to respond to and resolve new complaints/adverse events reported by clients.

Data security and reporting

- Ensure strict adherence to data protection regulations and organizational policies in the handling of client data. Emphasize the importance of confidentiality and security in all client interactions. Have a clear protocol for managing a staff person who does not follow these policies, including when termination should occur.

- Ensure that all workers sign a code of conduct that explains their responsibilities related to data security.

- Establish a routine reporting system for outreach workers to document their activities, challenges, and successes. This will provide valuable insights into the program's impact and areas for improvement.

Recognition and motivation

- Recognize the unique challenges faced by online outreach workers and implement strategies to acknowledge and reward their efforts. This could include regular recognition, incentives, or support mechanisms to maintain morale and motivation.

Support staff mental health and well-being

- Promote stress prevention and psychological health, ensure a harassment-free work environment, provide enough time to complete workplace tasks, and empower employees to participate in workplace decisions.

- Create space during team meetings to raise concerns or share experiences related to online or in-person harassment. Inform staff of protocols for reporting harassment and intentionally check in with staff to assess their current needs and concerns.

- Offer groups where workers can come together to discuss difficult cases (without identifying information) and the emotional aspects of their jobs. If possible, these can include food and time for social activities as well as time to process.

After an incident of online harassment, follow these steps:

- Reach out and listen to the affected employee. Reinforce that this is not their fault and ask what they need. Schedule a private check-in if you heard about the abuse from someone else.
- Offer support and applicable referrals to mental health services. Share resources available to them.
- Follow up with the employee and delegate responsibilities to others if they need to shift tasks to take a break from certain platforms.
- Assess the incident and apply further safeguards to help avoid a similar situation.

Additional resources

Annex 1 includes recommendations on how to adapt a broader range of telehealth approaches for more secure implementation of HIV programs in hostile settings. These recommendations extend beyond virtual client support to include marketing, referrals, case management, monitoring, and other areas of online outreach. Programs can also utilize these security and data security tools to assess their own security strengths and gaps and then act upon them in a thoughtful and strategic manner. These additional resources include a training designed for organizational leadership, a toolkit addressing security in several domains, and a dashboard and guidance on the security of strategic information specifically. Additional related external resources are also available (Annex 6).

Annex 1. Adapting telehealth approaches for hostile settings

FHI 360's Going Online framework presents a vision of applying telehealth approaches across the HIV services cascade. These virtual approaches can be used to expand outreach to previously unreached populations, support beneficiary engagement in program activities and services, and bring efficiencies to outreach and service delivery activities. This document outlines how programs in hostile settings can adapt and implement telehealth approaches in more secure ways, considering local security and population concerns. Most recommendations in this guide can be used to strengthen all KP HIV programs; however, those recommendations that may only be relevant or necessary for hostile settings are noted by an alert icon ⚠.

When determining whether each of these actions is necessary for your program, consider that security measures often have negative impacts on convenience, visibility, and cost. These negative impacts are often outweighed by the protections that come with implementing a security measure. For example, buying a phone that can be remotely disabled, adding a password to that phone, and limiting the data collected on KPs so that none is identified as a member of key populations could all be worthwhile trade-offs if the alternative is arrests of staff should the identifying information on a phone be accessed by someone wishing to do the program harm.

PLAN

Approaches to plan virtual and HIV interventions by learning about and engaging target audiences who use virtual platforms.

- ⚠ Implement approaches relevant for hostile settings, such as a legal analysis of laws affecting project participants and implementers, risk identification from the perspective of clients and all levels of staff, contingency planning for severe security events, and establishing a security team (see general preparation for hostile settings for more guidance).
- Use focus groups or ⚠ anonymous online surveys in hostile settings to learn from project participants. Avoid branding or limiting the survey to stigmatized audiences. Additionally, consult with local human rights and KP CSOs to understand the local legal and community context and guide planning efforts.
- ⚠ Avoid generating, compiling, or sharing sensitive data from, or about, online KPs that may result in harm to programs, clients, or KP communities, such as lists of social media pages, groups, and influencers where KP members can be reached; and estimates of online KP audience size.
- Solicit routine community input, including on unintended harms that may be occurring because of virtual programming, discreetly using community advisory boards or individual advisors. ⚠ Maintain contact individually and avoid group-based communications in hostile settings.
- Consider budget and only conduct virtual activities that can be done safely within the constraints of that budget. For example, in hostile settings, the best practice is for all outreach workers to use a device owned by the program, not their personal devices, for outreach. If the program cannot afford to purchase devices for workers, it may not be appropriate to use this modality.

REACH

Virtual demand creation for health services, including outreach and marketing efforts.

- ⚠ Avoid public-facing online demand generation activities specifically targeting KPs or try new campaigns from accounts with broader population focus, with inclusive messaging. Alternatively, revise all CSO-managed websites, social media accounts, pages, and groups to remove specific focus on KP in its public-facing mission, project description, posts, messaging, and branding. Some of these recommendations simultaneously pose the risk of "community erasure" and limiting the capability of communities and organizations to effectively advocate for the rights and dignity of KPs, and programs and communities will need to navigate these conflicting risks thoughtfully.
- ⚠ Avoid or be very cautious when creating and managing group-based communications for HIV outreach, such as Facebook pages/groups, WhatsApp and Signal groups, and other social media groups. Instead, consider taking steps under virtual communication guidance for joining external groups managed by people outside the program. Managing group communications with clients is not typically recommended in hostile settings. If this approach is implemented, admit new members after proper vetting, such as by confirming their identity and referral from an existing known member of the closed group and having an agreed upon and transparent process for admitting new members that all existing members are knowledgeable about and comfortable with.
- ⚠ Use individual online outreach that welcomes a broad audience while focusing on KP through targeted outreach, social networking, and individual trust-building with clients. Secure devices and apps for use by online outreach workers (see device management and security). Be ready to support broader audiences (non-KP) to access relevant services and education. Develop and implement communication guidance for online outreach workers (see

communication guidance). Use audio-only virtual consults and trust-building processes as an entry point to services.
- If online outreach workers first contact clients on other apps like social media platforms or dating apps, at the earliest opportunity, clients should be asked to contact workers on a secure messenger platform, such as WhatsApp, Signal, or Telegram. This will also make it easier to keep track of all messages and apply the standard security settings (see app and website security).

REFER

Link clients reached online to available health services.

Use secure virtual methods (such as ORA) to make referrals for clients to HIV education consultations, commodities, and other health services. The characteristics of a secure virtual referral mechanism are:

- Secure logins with user-level access for client support staff to view only the necessary client information.
- Encrypted databases and/or hosting the platform outside the country on a secure cloud server.
- Hidden client contact information on backend interfaces and data export.
- SOPs and policies that only allow assigned staff to view client contact information individually when they are providing virtual support.
- ⚠ In hostile settings, this platform should be presented in a health and population-generic way (not KP specific). Consider adding broader services and providers on the platform to avoid being identified as a platform only used by KP. Consider asking clients not to identify their KP status on the platform.
- Appointment reminders and other automated messages sent by the platform should use generic text without sensitive information related to specific health services or health or population status of the client.

DELIVER

Provision of health services and information to clients virtually.

- Have online outreach workers offer clients a virtual consult by voice call to build trust, provide HIV education and prevention messages, and understand clients' needs and necessary referrals. This can also be an opportunity to explain the ways in which the program will keep their data and conversations secure should they wish to be engaged in the program. ⚠ An audio-only virtual consult is recommended for all new clients reached online to develop trust before any in-person meeting, service delivery, referrals, or video-calls. Confirm client identity before starting consults and disclosing the CSO name or purpose of the call (see virtual communication guidance, section 9).
- ⚠ Identify alternative locations to provide in-person services to clients outside KP-exclusive CSO offices/DICs (which may risk the clients' security and privacy if they are seen entering or exiting).
- Offer clients the option to receive commodity-based services via home delivery using a third-party delivery provider, and be sure to pack commodities securely, exclude sensitive information on the outside of the package, and not communicate package contents to the courier. ⚠ Generate a code for the client to receive the package (known to the courier) to avoid the wrong person intercepting package

ENGAGE

Virtual approaches to keep clients engaged in health services to support retention, adherence, and other long-term health goals.

- Use a virtual case management approach to support clients in long-term care (e.g., routine prevention, PrEP, ART). Use a secure online platform to track client's service access and upcoming appointments (ORA).
- Confirm clients have private access to their mobile phone to receive calls and appointment reminders and discuss their communication preferences. ⚠ Turn on "disappearing messages" for chats with clients.
- ⚠ Use voice calls rather than messages to share sensitive health or population-specific content.
- Use automated or manual reminder messages for clients while ensuring these messages do not specify the services to be received, nor the health or population status of the client.

IMPROVE

Use of real-time data from outreach, service delivery, retention, and client/patient feedback for program improvement and knowledge sharing.

- Consider how to securely collect and store sensitive client data for program reporting. For instance, use a UIC on client records, which is de-linked from personally identifiable information. ⚠ Avoid collecting and storing KP status of clients on records where their identifiable information is also stored. In some cases, do not collect KP status at all or allow the client self-reporting of this information to be optional (see earlier guidance on Plan).
- Use secure systems to collect and store client information (e.g., logins, 2FA, secure hosting).

- Offer clients the option to provide feedback on their own device from the privacy of their home using an online survey format.
- Allow clients to submit their feedback anonymously.
- Program automated emails to send to program staff to receive and respond to new complaints submitted.
- When clients are providing their feedback/complaints, limit providers from being able to view feedback directly.

Annex 2. Sample training agenda

Time	Item	Participants	Format
8:00 a.m.	Training organizers arrive and secure training site, ensuring privacy		
9:00 a.m.	**Welcome and objectives** Note important disclaimers related to the security of the training and venue, how to discuss populations or topics discretely, etc.	Virtual client support staff	1-hour presentation
9:15 a.m.	**Pre-assessment** of existing knowledge and practices		Handout
9:30 a.m.	**Security overview** See "background" section of this guide.		
10:00 a.m.	**Activity: Risk identification and contingency planning** Break out into small groups of about five people to identify the three security risks most likely to occur to program implementers or clients communicating virtually. Consider steps to be taken if these risks occur.		Small group discussion and report-out • 10 minutes instructions • 30 minutes small group • 20 minutes report-out
11:00 a.m.	**SOP 1: Device management and security** See related section in this guide.		45-minute presentation 15-minute discussion
12:00 p.m.	Lunch break		
1:00 p.m.	**SOP 2: Virtual communication guidance** See related section in this guide.		45-minute presentation 15-minute discussion
2:00 p.m.	**Activity: Practice potential online outreach conversations** Role-play the following scenarios: • Initiate a conversation with a new contact referred by an existing client. • Respond to a client who messaged you based on an informational post you shared. • Respond to a client who reached out to you directly. • Respond appropriately to a security risk.		Role play/Discussion • Break into pairs, then report back OR • Selected individuals demonstrate and then discuss feedback or suggestions
3:00 p.m.	**SOP 3: Referring new clients to in-person services** See related section in this guide.		30-minute presentation 15-minute discussion
4:00 p.m.	**Closing remarks** Review Code of Conduct, clarify how to ask for help and where to find resources/guidance, and review other program data security, privacy, and safety guidance.		Presentation/Discussion
4:45 p.m.	Post-learning assessment		Handout
5:00 p.m.	Session end		

* Programs may wish to include specific sessions on (1) preparation activities (see earlier guidance), (2) broad communications/marketing, (3) broader organizational and community/personal safety and security.

LIST OF RESOURCES TO BE DEVELOPED FOR TRAINING:

- PowerPoint slides of technical guidance
- Pre and post assessment handouts
- Activity guidance
- Printed SOPs (a locally adapted version of this guidance)
- Code of conduct

Annex 3. Virtual client support staff terms of reference (sample)

The following is a sample terms of reference that describes the role of virtual client support staff and can be adapted for peer educators, online outreach workers, and case managers/peer navigators

Virtual client support staff conduct individual outreach and provide support to individual clients using online and virtual communication channels. They follow communication guidance to engage with new clients, build trust, and link them into the program and ensure they can access HIV services. They may also follow up with clients after they access services to ensure their ongoing sexual health needs are met.

ACTIVITIES

- Support existing clients' routine HIV risk screening and service access, and offer client referral options.
- Reach new clients online, including: (1) creating profiles/accounts on social media and dating apps; (2) engaging in group chats and social media groups and pages; (3) responding to client queries and service needs.
- Host virtual consults with new clients to establish trust, assess service needs, and make referrals.
- Maintain digital security for all online communications, inform supervisors of threats or hostile changes in the landscape, and follow protocols for referring new clients for in-person services.
- Support clients to request services by providing referrals, sharing links to book services on ORA, or booking appointments on behalf of clients.
- Support clients to access requested services by providing reminders and rescheduling missed appointments.
- Coordinate service delivery and routine client engagement with other staff, such as with service providers, delivery/courier services, or case managers.
- Securely meet clients to provide in-person support, conduct HIV testing, or provide other services.

MINIMUM QUALIFICATIONS

- Trained in basics of HIV and sexual health
- Member of the community and/or with special population-specific sensitivity training
- Can speak, read, and write in the nationally recognized language and language used by the target audience
- Proficient using smartphones and online apps
- Trained on online security guidance and digital security protocols for hostile settings

TECHNOLOGY REQUIREMENTS

- Internet-enabled smartphone, tablet, or computer
- Mobile data package (at least 2GB monthly data with calling and SMS credit)
- Apps for client communication: WhatsApp, Telegram, Signal, etc.
- Apps for outreach: Facebook, Instagram, Twitter, Grindr, Hornet, Blued, and others as appropriate
- Login and token link to book client appointments and assign cases on ORA

KEY PERFORMANCE INDICATORS

- Number of risk assessments completed
- Number of appointments/referrals made for HIV services
- Number of attended appointments/successful referrals
- Number of clients who received an HIV test and result
- [Add others based on expected activities and outputs.]

ADDITIONAL PREPARATORY TRAINING

- Social network outreach approaches
- Identifying and handling a catfish
- Processes for handling harassment and abuse online
- Digital security protocols
- Developing and maintaining a secure online and social media presence
- Use of ORA to help clients assess HIV risk, book services, arrive for appointments, etc.
- First-line response for gender-based violence (GBV) or intimate partner violence (IPV).

ADDITIONAL TOOLS

- Virtual client support guidance/SOPs
- Sample chat introductions and flows
- Contingency plan for online threats to staff
- Service directory to make service referrals

Annex 4. Virtual client support staff code of conduct (sample)

The following is a sample code of conduct for virtual client support staff that can be adapted for peer educators, online outreach workers, and case managers/peer navigators.

All virtual client staff must review and agree to this code of conduct to help ensure client confidentiality and privacy is maintained and security risks to clients, program staff, and organizations are minimized and mitigated. As failure to comply with this code may result in in harm to the staff, damage to the organization's reputation, or threats to client security, disciplinary measures may be taken. By adhering to this code of conduct, we demonstrate our commitment to upholding the highest standards of professionalism, ethics, and integrity in our virtual client support roles within the HIV program.

CONFIDENTIALITY AND PRIVACY:

- **Client Confidentiality:** We understand the sensitive nature of the information shared by our clients regarding their HIV status and related health issues. Therefore, we commit to maintaining the utmost confidentiality regarding all client information.
- **Data Handling:** We will handle client data with care, ensuring that it is stored securely and accessed only by authorized personnel for the purpose of providing support services.
- **Privacy Protection:** We will always respect the privacy of our clients, refraining from discussing client cases or sharing any identifying information with unauthorized individuals or entities. We will refrain from providing virtual support to clients when in locations without adequate privacy and secure internet connections.

DATA SECURITY:

- **Secure Communication:** We will use secure channels of communication when interacting with clients, ensuring that sensitive information is transmitted safely and encrypted where necessary.
- **Data Storage:** We will store client data in secure databases or platforms that comply with organizational standards.
- **Access Control**: We will not share our login credentials or access to the apps we use to interact with clients or collect their data with unauthorized individuals or entities. We will use strong passwords and authentication methods to prevent unauthorized access.

DEVICE SECURITY:

- **Device Protection:** We will ensure that our devices used for client support are not left unattended and stored in secure locations when not in use.
- **Password Protection:** We will set strong passwords for our devices and accounts, refrain from sharing them with others, and change them regularly to minimize the risk of unauthorized access.

RESPECTFUL COMMUNICATION WITH CLIENTS:

- **Empathy and Sensitivity:** We will interact with clients in a respectful, empathetic, and nonjudgmental manner, acknowledging the challenges they may face and offering support without discrimination.
- **Clear Communication:** We will communicate information clearly and effectively, ensuring that clients understand their rights, the services available to them, and any actions required on their part.
- **Active Listening:** We will actively listen to our clients, validate their concerns, and provide them with the opportunity to express themselves without interruption or judgment.
- **Separating work from personal life:** We will use our nickname in all communications with clients and protect our own privacy. We will refrain from using personal services and profiles to communicate with clients. We will not engage in romantic/intimate relationships with clients.

COMPLIANCE AND ACCOUNTABILITY:

- **Adherence to Policies:** We will adhere to all organizational policies and procedures related to client confidentiality, data security, and respectful communication, seeking guidance from supervisors when faced with ethical dilemmas or uncertainties.
- **Continuous Improvement:** We will continuously seek opportunities to enhance our knowledge and skills in client support, staying updated on best practices and emerging technologies to better serve our clients and safeguard their privacy and security.
- **Reporting Violations:** We will promptly report breaches of confidentiality, data security incidents, or instances of disrespectful communication to our supervisor or security team, taking responsibility for our actions and working toward resolution and prevention of future occurrences

Printed name: _____ Signature: _____ Date: _____

Annex 5. Sample client terms of use policy (for ORA/QuickRes)

[Note: This is a draft terms of use policy for clients using QuickRes. This global template should be adapted to the context of each country/project using QuickRes. Attention should be given to adapting sections in red font.]

QuickRes allows any member of the public to find and book appointments for a range of health services in their country. Booked appointments are shared with relevant service providers and client support staff who may assist clients to attend their appointments and document the health services provided to those who had booked on QuickRes. [This statement should be adapted to country-implementation context.]

QuickRes (available at www.quickres.org) uses the Online Reservation and Case Management App (ORA) software developed by FHI 360 with funding provided by USAID and PEPFAR. QuickRes is available in several countries and languages. QuickRes is operated by FHI 360 — an international nonprofit working to improve the health and well-being of people in the United States and around the world. FHI 360 and local project partners [list partners] are considered the "controllers" of QuickRes in [country] (available at https://quickres.org/[CountryToken]).

We are committed to protecting and respecting your privacy. We collect and process your personally identifying information (PII) in accordance with national and local laws. We continually try to minimize the amount of private data that we collect. All clients who use QuickRes indicate that they have read, understand, and agree to these Terms of Use. Our Terms of Use explain what client data is collected on QuickRes, why we collect this information, and how it is processed securely.

Contents:

Key terms:

- **Personally identifying information (PII):** Information that can be used to uniquely identify, distinguish, or trace an individual's identity, such as name, phone number, email address, date of birth, location, IP address, and device ID. PII can also extend to include information that is linked or linkable to an individual such as medical information, sex, gender, and population type. PII is also referred to as "your information" in this policy. Aggregate data or individual level data that cannot be linked to an individual are not considered PII.
- **Controller:** The entity or entities which, alone or jointly with others, determines the purposes and means of the processing of personal data on QuickRes. FHI 360, as the global administrator, and relevant in country program partners are the QuickRes controller and are referred to as "we" in this policy.
- **Clients:** Any individual who uses QuickRes to book health services for themselves or for whom appointments are booked on their behalf by service providers or client support staff. Clients are also referred to as "you" in this document.
- **Service providers:** Providers of health services registered on QuickRes, which may include clinicians, nurses, qualified community/lay providers, lab technicians, counselors, psychologists, pharmacy staff, and other individuals who are qualified to provide the health services clients request when they book appointments on QuickRes. Service providers have access to view appointments booked on QuickRes at the service provider's clinic(s) to report when clients arrive for their appointment and report services provided to clients. [Adapt statement based on program implementation context.]
- **Client support staff:** individuals who are assigned access to appointments booked on QuickRes and may include "outreach workers" who help reach new clients in the community and assist them to book services on QuickRes. This may also include "case managers" who usually manage a cohort of clients in longer term care and may have access to the history of appointments their clients booked on QuickRes including clinical service delivery data reported by service providers. [Adapt statement based on program implementation context.]

How do we collect your information?

- You directly enter your information on QuickRes when you book an appointment on QuickRes, including your mobile phone number, date of birth, and name (or nickname). Service providers use this information to confirm your identify before providing virtual or in-person support. QuickRes will use your mobile number to send you appointment confirmation and reminders by SMS.
- QuickRes automatically collects limited information when you visit QuickRes, such as your IP address, general location (city and country), time of visit, and the type of

device and operating system used to access QuickRes, which is used to understand site traffic.

- You may request assistance from service providers or other client support staff to book your appointment on QuickRes on your behalf. In this case, you may have your information entered into QuickRes by service providers or client support staff after this information is confirmed by you.
- You may refer other individuals for services on QuickRes using the client referral tool. Alternatively, you may be referred for services on QuickRes by someone else. Clients making the referral will enter the mobile phone number and name/nickname on QuickRes for each client they want to refer. [Remove this statement if the client referral function is turned off for the country.]
- Your assigned client support staff and the service provider where you booked your appointment may collect additional information and report it on your appointment records on QuickRes. This may include whether you arrived for your appointment and information about the health services you accessed during your appointment. Learn more about what kind of information is collected in QuickRes in the section below.

What kind of information do we collect and how do we use your information?

- **Appointment information:** Your name (or nickname), mobile phone number, date of birth, and the health services you want to receive are collected when you book an appointment on QuickRes. This information is used to send you reminders for your upcoming appointments and allows QuickRes to share your appointment details with the service provider where your appointment was booked and your assigned client support staff. It helps service providers and client support staff find your appointment record on QuickRes and confirm your identity and requested services.
- **Other demographic information:** Additional demographic information may also be requested when you book an appointment on QuickRes, such as sex, gender identity, and membership in some populations, which allow us to ensure all populations are served equitably.
- **Sexual health information:** You can complete a sexual health service assessment on QuickRes, which asks a series of questions to determine your HIV status and risk level for HIV and other STIs. Your responses to these questions allow QuickRes to recommend specific health services that you can book on QuickRes. Your responses to individual questions on this assessment are kept confidential and are neither shared with service providers nor client support staff.
- **Health service access information:** Your service provider and/or client support staff assigned to your appointment record may report the health services you accessed and diagnostic results based on the appointments booked through QuickRes, including ability for them to add custom notes. This information is collected to ensure clients are provided comprehensive quality health services and to allow case managers to understand their client's history of service uptake among providers on QuickRes. [Remove this statement if clinical service provision will not be collected on QuickRes.]
- **Client feedback information:** You may be offered the option to provide feedback on your appointment booked on QuickRes. This information is to understand your experience accessing services through QuickRes to improve the quality of services.
- **Client referral information:** QuickRes collects the phone number and sex of each contact as well as specific health services that should be offered for each contact entered on the QuickRes client referral tool. This information is used to send an SMS message to each referral and to track details of referrals sent by QuickRes. This information is also shared with an assigned client support staff member and service provider on QuickRes so they may manually follow up with referred clients to support them to access services through QuickRes.
- **Location information:** The internet browser you use to access QuickRes may ask your permission to share your current location with QuickRes. This information is not stored on QuickRes but is used to personalize your experience using QuickRes, including to present service providers that are nearest to your current location.
- **Cookies and other tracking information:** When you visit QuickRes, the site will automatically collect some information to help us understand our site traffic, including your IP address, general location (country/city), device type, and date and time of access.
- We do not use client data for prospective and commercial uses. [This statement may need to be adapted for a country if there are private fee-based providers on QuickRes and they intend to use client data for marketing purposes.]

How is your information shared?

- Your appointment requests are shared with the provider where you booked your appointment and the assigned client support staff. This service provider and assigned client support staff can reassign your appointment record to another service provider or client support staff based on your request and approval (for instance, if you want to change your appointment to another clinic).
- Clinical data, including details of the health services you accessed and diagnostic results based on your appointment booked on QuickRes can only be viewed and edited by the provider where your appointment is booked. Your provider may also grant access to another provider on QuickRes to complete reporting of certain diagnostic or drug delivery for your appointment on QuickRes (such as when your provider will grant a laboratory access to your appointment record to report diagnostic results or grant access to your appointment record to a pharmacy to allow them to report they dispensed drugs to you). [This statement should be removed if no clinical data will be reported. This statement should be edited as necessary to denote if other users will be granted access to view/edit

the clinic reporting buttons on client's appointments, such as by the assigned outreach worker or case manager.]

- QuickRes does not share your personal information to any other database or national/government reporting system. Only aggregate and anonymous data may be shared and reported to the national government and donors, upon request. Based on regulations established by the Ministry of Health, providers may be required to report data on delivered services to the national government, but that would be handled by your provider and not on QuickRes. [This statement should be adapted to the local context.]
- Program staff may use aggregate appointment data (without client identifying information) to help ensure all types of populations can access and receive services through QuickRes.
- Clients agreeing to the QuickRes Terms of Use provide their consent to having their information transferred outside of [country] to QuickRes' secure cloud server, where the QuickRes controllers have access to your information to provide management support to service providers and client support staff.

How do we protect and secure your information?

We take great care to protect client data. Technical measures are in place to prevent unauthorized or unlawful access to data and accidental loss, destruction of, or damage to data. Staff who are granted access to QuickRes data are trained to protect the data from any illegal or unauthorized access and usage. We protect and secure your data in the following ways:

- Trained management, outreach, and counseling staff carefully support clients and handle their information securely. Our clinical partners are nationally accredited and follow health information guidelines set by the Ministry of Health.
- QuickRes uses a range of security measures to protect clients and data including using Secure Sockets Layer, which encrypts your communication with QuickRes, secure high-capacity server hosting, off-site backup service with military grade encryption, and password-protected user logins.
- Your phone number used to book appointments on QuickRes is protected on QuickRes. The phone number is encrypted on the server and hidden from view of providers and client support staff. QuickRes uses a key to decode the phone number each time it is required for use (to send clients SMS reminders or to present the phone number to the service provider or client support staff to contact you). QuickRes' databases do not link your personal information with your phone number. [Phone number encryption is part of QuickRes v4.2.]

What kind of communication will you receive from QuickRes?

You may receive the following types of communications from QuickRes:

- One appointment confirmation SMS message is sent to the phone number included on the QuickRes appointment immediately after the appointment is saved on QuickRes. The message will not include the specific health services you requested for your appointment.
- Two reminder SMS messages are sent to the phone number included on the QuickRes appointment. The first reminder message is sent 48 hours before the scheduled appointment, and the second message is sent 24 hours before the scheduled appointment. These messages will not include the specific health services you requested for your appointment.
- One follow-up SMS message is sent to the phone number included on the QuickRes appointment at 6 p.m. local time on the date of the scheduled appointment. This message contains a link to an online survey where you can provide feedback on your appointment. The message will not include the specific health services you requested for your appointment. [Remove #3 if the client feedback SMS function is turned off for the country.]
- One SMS message is sent to the phone number included on the QuickRes appointment when a change is made to the appointment's date, time, provider, or assigned client support staff.
- One SMS message is sent to each phone number entered on QuickRes' client referral tool. This message includes an invitation to access services on QuickRes and may recommend specific health services to the client. The message will not contain information about the person who referred the client using QuickRes' client referral tool. [Remove this statement if the client referral function is turned off for the country.]
- One SMS message is sent to the phone number included on the QuickRes appointment when diagnostics are reported by the laboratory or lab specialist, including instructions to call to learn about your result. The message does not include information about the specific health services or results. [Remove this statement if the function for sending SMS for updated HTS and VL results is turned off for the country.]
- SMS messages are sent from QuickRes as part of planned SMS campaigns relevant to health services you have accessed through QuickRes or to share updates on health services available through QuickRes. [Remove this statement if the SMS blast function will not be used in the country or turned off.]
- Voice call, SMS, or WhatsApp message/call may come from the service provider where your appointment is booked or from another client support staff who is assigned access to your appointment. They may call you to confirm your appointment, assist you, to reschedule to another date/time, or to collect information from you prior to your appointment. The provider/client support staff should confirm their identity first and ask you to confirm your identity by confirming your name/nickname and birthdate used on the appointment before discussing personal or health matters.

How can I edit my communication preferences and opt-out of QuickRes' communications?

- Select “opt out of SMS” when you book an appointment on QuickRes or request the provider or client support staff select this option when they book an appointment on your behalf. Selecting this option will block QuickRes from sending you automated SMS messages for that specific appointment (will not affect other automated messages sent for separate appointments).
- Select “do not call” when you book an appointment on QuickRes or request the provider or client support staff select this option when they book an appointment on your behalf. Selecting this option will notify the service provider and other client support staff to avoid contacting you on the phone number you provided and to take extreme precaution to confirm your identity if contacting you is necessary.
- Contact your service provider or case manager to have your phone number updated on QuickRes or to provide them custom contact information (such as WhatsApp number or other contact information).
- To stop receiving all SMS from QuickRes, please contact us using the email or phone number at the bottom of this Terms of Use. We can manually and permanently block all SMS from QuickRes to your phone number.
- When you receive an SMS from QuickRes, it will include a phone number that can be called or texted to opt out of future communications.

How can you manage or delete your information on QuickRes?
We provide you with the ability to access, rectify, or delete your data. You can manage your date through the following:
- Call the phone number provided in your appointment booking confirmation SMS from QuickRes to rectify or delete your data.
- Start a chat with us on the home page and ask to speak to your assigned client support staff, who can help you access, rectify, or delete your data on QuickRes. When you start a chat with us on the home page, the chat is facilitated by WhatsApp, Facebook, Telegram, and/or Viber. [Adapt statement to specify only the chat platforms used in country.]
- Meet with your service provider in person during your appointment booked on QuickRes and ask them to rectify/delete your data.

Requests to access, edit, or delete your personal data on QuickRes may only proceed after service providers or client support staff can confirm your identity. After your identity is confirmed, requests will be processed within 10 days. If you cannot submit your request to manage or delete your personal information in QuickRes with the options described above, send an email with your request to privacy@fhi360.org.

What is the minimum age to use QuickRes?
If you are [insert minimum age limit for the country] or older, you may use QuickRes to book health services for yourself. If you are younger, you can ask your parent or legal guardian to book health services on your behalf. On the final page to book an appointment on QuickRes, parents can respond to the question “I am booking an appointment for…” by selecting “my child.” No proof of age will be required for you to book an appointment on QuickRes, however, the service provider may request proof of age (such as identification card) and may refuse to provide services if it is illegal for them to provide such services without parent or guardian approval/presence.
FHI 360 will not be liable for any cause of action that arises due to non-compliance with this section.

How can you contact QuickRes/FHI 360 with questions?
If you have questions about this policy, you can contact us as described below:

[Name of local controller] (Local QuickRes controller)
- Contact us by email at: [insert email]
- Contact us by phone at: [insert phone]
- Our officers are located at: [insert local office address]

FHI 360 (Global QuickRes controller)
- Contact us by email at GoingOnline@fhi360.org
- Requests to modify or delete client personal information can be sent to privacy@fhi360.org
- FHI 360’s office is located at: FHI 360 Headquarters, 359 Blackwell Street, Suite 200, Durham, NC, 27701, US
- FHI 360 is committed to making our programs safe for everyone. Please let us know if you ever feel uncomfortable or hurt by anyone from FHI 360, including anyone who works with one of our partner organizations. You can send an email to compliance@fhi360.org, report a case anonymously online here, or call FHI 360’s hotline +1.720.514.4400. FHI 360 commits to non-retaliation for anyone who submits a report.

Annex 6. Additional resources

- FHI 360. Technology-facilitated gender-based violence orientation. 2024. Available upon request – email Jennifer Arney, JArney@fhi360.org.
- FHI 360. Security assessment tools including (1) threat assessment questions, (2) security planning template, and (3) a security checklist. 2024. Available upon request – email Robyn Dayton RLDayton@fhi360.org.
- FHI 360. Ensuring safe and inclusive spaces: GESI and safeguarding tips for local organizations. 2023.
- FHI 360. Security toolkit: Protecting implementers and improving program outcomes. 2022.
- FHI 360. EpiC implementer and data security. 2021.
- FHI 360. Community-led monitoring resources. 2021.
- FHI 360. Secure use of mobile devices and apps: A guide for HIV programs providing virtual client support. 2021.
- CivicSpace.tech: an interactive resource to ensure use of digital technology does not undermine development solutions. See data protection section.
- SafeQueers. Empowering LGBTQ+ organizations in at-risk areas to protect themselves digitally.
- Norton. Catfishing warning signs and protection tips. 2022.
- Harvard School of Public Health. Digital Safety Kit for Public Health.