Meeting Targets and Maintaining Epidemic Control (EPIC)
Cooperative Agreement No. 7200AA19CA00002
VERSION 1 | MAY 2021

Secure Use of Mobile Devices and Apps

A GUIDE FOR HIV PROGRAMS PROVIDING VIRTUAL CLIENT SUPPORT

PEPFAR
USAID FROM THE AMERICAN PEOPLE
EpiC Meeting Targets and Maintaining Epidemic Control

Secure Use of Mobile Devices and Apps: A Guide for HIV Programs Providing Virtual Client Support

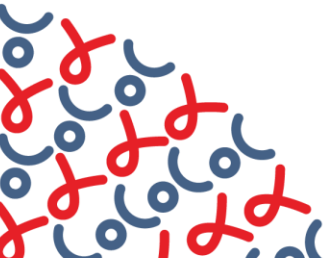
Version 1 | May 2021

This guide 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, Population Services International (PSI), and Gobee Group.

Recommended Citation:

FHI 360, EpiC Project. Secure Use of Mobile Devices and Apps: A Guide for HIV Programs Providing Virtual Client Support. Washington, D.C., U.S.: FHI 360; 2021.



Introduction

With an estimated 67% of the world's population using a mobile phone and 59% having internet access in 2020,[1] virtual platforms have become ideal channels to reach and maintain contact with potential and current HIV service beneficiaries. This is particularly true for basic phone calling, short message service (SMS), and commonly used internet-based messengers such as WhatsApp, Facebook messenger, and Telegram. The COVID-19 pandemic has further solidified the role of virtual platforms for ensuring continued access to HIV services. As a result, almost all HIV programs are either beginning to use or increasingly relying on virtual connections to support activities that range from prevention messaging, risk assessment, and service booking and provision to result sharing and case management.[2]

Each element of virtual HIV service delivery carries risks and rewards; both should be contemplated, and risks mitigated in a systematic and careful manner as services are initiated or scaled up. This guidance is to assist organizations with the selection and management of mobile devices and apps for staff members who provide virtual client support such as outreach workers, case managers, and clinical staff. Topics include accessibility, affordability, and functionality with special emphasis on security and mitigating risks. Specific considerations are provided for workers who engage with key populations virtually and for programs that collect data related to online service provision for quality improvement.

Please note that this guidance is written to describe a rapidly evolving space. As technologies advance and malware, viruses, and hacking schemes morph, it is important to keep up-to-date on both the risks and solutions most likely to be relevant to your organization's efforts. This guidance cannot be considered exhaustive. In particular, this guidance does not cover telemedicine, the delivery of clinical services via virtual platforms such as diagnosis. Instead, it focuses on outreach, booking, and case management.

Contents

1. Choosing Devices

This section reviews some considerations when deciding which mobile devices to procure for staff who are providing virtual client support.

Important: Basics of choosing devices

The devices and accessories you choose will impact the level of security of your communications, as well as the ease and types of communication possible. A great deal of sensitive data may be exchanged online and stored on mobile devices used for online HIV outreach. Even when conversations are not stored on these devices, clients can be exposed to harm if their contact information is accessed by third parties with malicious intentions.

When insufficient consideration is given to the model, vendors, and technical specifications of mobile devices, programs run the risk of:

- Purchasing security-compromised devices from vendors who have altered the operating systems.
- Exposing client information on devices that are not adequately furnished with strong user-enabled security features and screen privacy.
- Having limited capabilities to secure and retrieve data from devices that become faulty or are lost or stolen.
- Increasing the likelihood of theft because of the device's popularity and resale value.
- Losing control over who speaks officially on behalf of your project.

1.1 Type and Size

- Purchase devices that are not locked to a single carrier. This will allow you to use, and switch between, any mobile network if charges become expensive or privacy terms become unfavorable.
- Smartphones are ideal because they can run many apps to communicate with clients, in addition to voice calling/SMS or program reporting tools. Smartphones also tend to have stronger security features such as thumb print, face ID, and unique pins or patterns.
- Staff using devices only to stay in contact with clients can use smartphones with a screen size of about 5 inches.
- Staff using devices for reporting, case management, or client tracking need a larger screen size (7 inches or more)[3] for easier navigation of the app tools.

- Consider Android devices for outreach workers because of their simple interface. They are also more interoperable with useful Google products and applications. Standard security protections include user-enabled app permissions and pattern, pin, and biometric security and protection of USB device serial number. (For more on Android security, see this article). iOS or Apple devices also have these strong security features and others such as a secure cloud ID that acts as two-factor authentication. (For more on Apple iOS security, see this article). However, iOS devices are often more expensive than Android ones, increasing the chance of theft.
- Do not purchase "rooted" or "jailbroken" devices. These give full access to a device's operating system and features to malware authors who can leak, sell, and destroy data. For more on security of jailbroken devices, see this article. Do not jailbreak or root devices after they have been purchased. Organizations that have already purchased rooted or jailbroken devices must ensure that an antivirus software is installed and that only apps from the app store are installed to prevent malicious attacks (for related information, see this article or this article).
- USG-funded HIV programs and funding recipients must not buy devices from Huawei, ZTE, or their subsidiaries because of U.S. government policy (Section 889 of the National Defense Authorization Act) that restricts USG funds from being used to procure devices and services from these companies (for related information on section 889, see this article).

1.2 Usability, Storage, and Connectivity

- Consider purchasing devices with a built-in memory of at least 16 GB to run essential apps. Depending on the operating system and brand, you may be able to add more space using an external memory card. Whether an external memory card can be used, and the appropriate type, will be detailed in the product description.
- Choose a tablet able to connect to the internet. Ensure the tablet has a SIM card slot to allow for mobile data connection for field-based internet access and voice calling. Tablets without SIM cards may be limited to Wi-Fi-only internet access, which may have limited range, inconsistent connection, or may not allow standard voice calling.
- Teams that generate and monitor social media content may find value in acquiring a device with a good quality camera and enough gigabytes to manage social media apps. Most modern mobile phones and tablets have these features.

1.3 Power Needs

- Consider devices with long battery life, especially if they will need to be used over long hours without access to a power supply for recharging.
- Purchase portable power sources such as a power bank to ensure devices are always charged during field work and in the event of prolonged power outage.

1.4 Vendors

- Purchase devices that use the same operating system (iOS or Android). This will shorten the learning curve for those using the newly procured devices. In addition, hardware can be shared if cables, cases, or other items become damaged or lost.

- Look for vendors that offer warranties and other post-sale services, which will be useful if issues arise with the devices you purchase. Be sure to document and store vendors' information and receipts.
- Do not purchase pre-owned or refurbished devices. If not purchased from a reputable vendor, pre-owned devices could be security compromised with several complications such as faulty screens and audio or an unauthenticated operating system. Organizations that have already purchased pre-owned devices must ensure that an antivirus software is installed and that only apps from the app store are installed to prevent malicious attacks.

1.5 Donated Devices

- Mobile devices received as donations should be carefully assessed by inspecting the screen and lock/power buttons and checking for existing personal data and apps. When deciding whether to use such devices, also consider the durability and lifespan to ensure compatibility with the latest versions of various apps used in online HIV outreach. For more on planning mobile device distribution, see this article.
- Delete existing applications and data if a device was previously used by staff in another program. Restoring factory settings is one way to ensure that all previously added information and applications have been removed. For more on restoring devices to factory settings, see Android devices and iOS devices.
- If SIM cards were left inside the donated devices, remove and replace them with others procured/owned by your organization. Do not use a number previously owned by someone else, especially when setting up messengers such as WhatsApp or Telegram.
- Have a clear policy about what donations your organization accepts. This policy should outline the hardware specifications described in section 1.1 above, and the preferred operating system. It should also describe steps for adding these devices to your inventory and safely passing them off if they will not be used by your organization. For more on how to accept or refuse donations, read this article.
- Be sure to request and store any documentation that comes with the donated devices. It may prove useful when troubleshooting issues and capitalizing on post-sale warranties or support.

1.6 Peripherals and Accessories

- Purchase SIM cards on behalf of staff to prevent them from owning the phone number assigned to their device. This makes it easier to reassign devices and numbers when staff changes occur. This is particularly important if a staff person becomes disgruntled or is asked to leave the organization, as they can immediately be removed from official communication lines. Consult with local network providers about options such as closed user groups (CUGs).
- Smartphones are likely to have a built-in camera and keyboard, limiting the need for connection to external input devices.
- While tablets can accommodate an external keyboard and mouse, not using them makes it easier to transport, store, and sanitize such devices.
- Furnish each mobile device with a durable case and a screen protector not only for protection from damage but also to keep them looking new.

- Consider purchasing privacy screen protectors of tinted tempered glass, if available, instead of transparent ones. They allow mobile devices to be used privately and in public places without revealing confidential information. The user can see the information being displayed, but others on either side of them will only see a darkened screen. This is particularly important if the worker will be using the device in the field or at home instead of a project office.
- Purchase a device case and a bag to carry the device in the field. A case is particularly useful if the device will be handed to clients to enter data. However, nothing carried by workers should indicate that a device is inside, as this may increase the probability of theft.

Pro tips for virtual client support staff

- Workers should only use devices provided by their organizations. Any use of personally owned devices must be approved and noted by management. Workers using their own devices should only engage in official activities when using a SIM card provided by the organization.
- Workers using devices purchased by the program must use the provided carrying cases and screen protectors.
- Only use original charging accessories purchased from a trusted manufacturer. Do not use public USB charging stations and never connect devices to government computers, whether via cable connection, Wi-Fi, or Bluetooth.
- If an individual is using a mobile device and a call comes in for another outreach worker, have that worker accept the call if they are available. If they are not available, inform the client that the worker is not close by and offer a call back.
- If outreach workers must share devices, they should ensure they have logged out of each of their social media/dating app accounts before handing the device to another worker.
- Workers should not access conversations that are not assigned to them.
- Workers should not store personal details, bank cards, banking information, or images of themselves or clients on the devices.
- Workers must advise clients if the mobile number/device is being used by multiple workers. This can be stated during initial engagements, for example: “Everything you share with me is kept safe, but other workers may receive calls or messages from their clients on the phone I am using” or as an automated response on apps like WhatsApp. For more on crafting an away message, read this article.

2. Deploying and Managing Devices

This section provides guidance and steps for preparing devices and deploying and managing their use among staff who provide virtual client support.

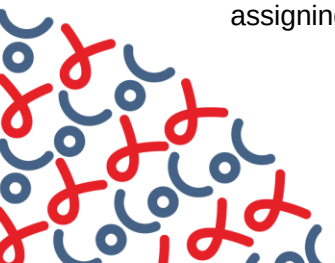
Important: Basics of deploying and managing devices

From creating passwords and profiles to downloading and installing apps, there are always potential security threats. Program teams must take care when setting up mobile devices by being deliberate about email addresses, profile details, and apps used for online outreach. The operating software on mobile devices should be regularly updated, and management should always be able to account for all the devices distributed to staff. Ignoring these security measures could result in:

- Malicious attacks and data leaking enabled by unsafe third-party apps and internet access.
- Workers and clients being harassed because their identities were not protected in vulnerable or user-anonymous online spaces.
- Data loss when devices are not periodically backed up or have the most up-to-date version of operating software and apps installed.
- Unretrievable mobile devices that are stolen, become faulty, or are lost. In cases where there is poor inventory procedure, programs may not be aware when devices have been taken from their facilities or not returned when a worker has left the team.
- General misuse and poor care of devices used in online HIV outreach.

2.1 Setting Up Devices

- Organizations may consider using a mobile device management (MDM) platform to set up and routinely manage devices. 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 international not-for-profit and trusted 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.
- If not using an MDM, check that each device's 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. If not, follow the steps below to run software updates before installing applications and assigning devices to staff:



Android devices:

1. Plug the device into power and connect to the internet with Wi-Fi.
2. Open the phone's Settings app.
3. Near the bottom, tap System > Advanced > System update.
4. You will see your update status. Follow any steps on the screen.
5. For more information, see this article for Android devices.

iOS devices:

1. Plug the device into power and connect to the internet with Wi-Fi.
2. Go to Settings > General, then tap Software Update.
3. Tap Download and Install. If a message asks to temporarily remove apps because the software needs more space for the update, tap Continue or Cancel. Later, iOS will reinstall apps that it removed.
4. For more information, see this article for iOS devices.

- Use the organization's name as opposed to a staff member's name when setting up mobile phones. Do not upload any images of staff or clients in the phone's user profile. Such photos could put workers or clients at risk if they could be identified as members of key populations, as people living with HIV, or targeted for harassment or stalking.
- Install an antivirus software such as Avast or Endpoint Security, especially for devices used for case management. Regardless of the software used, management will need to periodically monitor virus signatures and applications while addressing any flagged infections. This is to be done when the devices are occasionally assessed; it can be done using an MDM.

2.2 Creating Passwords and Screen and SIM Locks

- Using only a pattern or pin password—not a fingerprint or facial recognition—is best for safety and security. Patterns and pins are more secure than face or fingerprint (biometric options) as they are less possible to access without the user's consent (e.g., with face ID, it is possible to put a phone in front of the owner's face and unlock the device without their permission). Local laws will also determine whether law enforcement may require a detained individual to unlock their phone; in some contexts, this depends on the type of lock used.
- Create a pin to complement biometric options to safeguard against lockout.
- Do not use simple or predictable phrases or numbers when creating passwords or pins. Use longer instead of shorter codes when offered this option. Create pins using four digits or more. Longer pins are generally more secure and difficult to crack.
- Ensure supervisors have a record of device passwords. Ensure the passwords are stored safely in a password-protected database that few people have access to.
- Set up a pin code for each SIM card, which will require pin confirmation for the SIM to be activated on another device (typically this is found under SIM settings, which may appear in the phone settings).

- Some apps may require a password, such as social media or dating ones used in online outreach. If not using an existing account created for the organization, be sure to create strong passwords. Follow the steps below:
    - Include at least 8 characters
    - Include a mix of numbers, symbols, capital letters, and lower-case letters
    - Do not use dictionary words or a combination of dictionary words such as “Red House.”
    - Do not use the same account name and password anywhere else.
- When creating accounts for apps that require an email address, use one assigned by the organization. This will allow subsequent users to be able to change the password.
- Staff should never share passwords with other workers who do not require access to an account or device not assigned to them.
- Think carefully about security questions and answers if they are required when creating an account. Document them and keep them safe with a supervisor or information technology (IT) manager.
- Whenever available, use two-factor authentication for applications and websites (e.g., the user must enter a password and receive a code at a given phone number).
- Change passwords every 12 months for an added layer of security.
- Note that when you set up your passcode, there may be an option to erase data after too many failed attempts. If this option is selected, the device will erase all the data after a number of failed passcode attempts. The data will no longer be available on the phone, but if it was backed-up to the cloud, it can be downloaded later.

2.3 Downloading Apps

- Use the device’s official app store when adding apps. This varies based on the device’s operating system. Do not download unknown apps (apps not found in app store) because they are less regulated/accountable and more likely to compromise client data. See one caveat below regarding .apk and .ipa files.
- When downloading an app, carefully review the permissions required by the app to function. These permissions may include:
    - Location (do not enable or allow)
    - Contacts
    - Calendar
    - Messages
    - Microphone
    - Camera
    - Photos/media/files

- Change permissions at any time using the device's settings feature

- Some permissions may not be able to be changed. For example, WhatsApp does not allow the user to turn off data sharing with parent company Facebook. So, while Facebook does not receive the content of messages on WhatsApp (which are encrypted end-to-end) it does share how often you use WhatsApp, how you interact with other users, your operating system, app version, time zone, language used, and mobile network used.[4] Use this knowledge to select apps that share only information you are comfortable providing.

- There is one exception to the rule regarding use of the official app store. Users may download an internally approved .apk or .ipa file. These may include custom apps or software designed for case management or online outreach. The .apk or .ipa files must first be downloaded to a computer (with antivirus installed) and then transferred to the device using a USB connector cable. You may be required to temporarily disable security features that block the installation of third-party apps that are not from the app store. You must restore these permissions to their original state after installation. Note that cyber criminals may try to lure users into downloading an .apk or .ipa file for a common app by suggesting that premium features have been disabled for that version or that additional security has been added.

- Reference table 1 for some recommended apps used for online HIV outreach.

Table 1: Mobile applications for virtual client support

TYPES	OPTIONS
Reaching New Audiences Use these apps to reach new audiences online with HIV prevention information and services. These apps store user information in a secured cloud space and not on the mobile devices. Accounts are password protected, so once the worker logs out of their account, the data cannot be accessed. They each allow users to start private chats, but Facebook requires the installation of the Facebook Messenger app for private chats on mobile devices.	■ Facebook ■ Instagram ■ Twitter ■ Tik Tok
Reaching Key Populations In contexts where there is high-stigma, these dating apps normalize user-anonymous profiles. Community staff who use these platforms, can also confidently have anonymous profiles as they engage new clients online. It can be hard to verify who you are talking to and so there is a lot that goes into building trust before clients agree to enter the facility for services. Platforms like QuickRes make it easier for clients to book appointments at their own pace and may never have to reveal their identities. Some clients may ask to move the conversation to another messenger app where they feel safer to share additional information. These dating apps are also password protected by design and may include additional security features to hide the app and its contents and protect vulnerable users. For example, in addition to having a decoy for their app,	■ Grindr ■ Adam4Adam ■ Blued ■ Jack'd ■ Hornet

Grindr disables geo-location features for countries with a history of violence against lesbian, gay, bisexual, transgender (LGBT) people.[5]	
Staying in Touch These apps are quite useful for keeping in touch with clients or providing virtual support. While they may have cloud back-up features, they store the data exchanged between clients and workers on the device itself. Telegram, WhatsApp, Line, and Signal do not have options to 'sign out' of your account. Deleting these apps will remove the settings and data from the device, which can be restored if backed-up to the cloud. Users can sign out of desktop sessions online or using the mobile apps. WhatsApp, Signal, Telegram, and Line also have end-to-end encryption that prevents the conversation from being intercepted by a third party. WhatsApp and Telegram have 'disappearing' or 'secret' messages that become unavailable after a certain period. This would have to be enabled for each contact. Most devices come with a default SMS app that allows users to exchange text, image, and sometimes voice messages with carrier fees. iOS users can send messages to each other at no cost using iMessage. Default voice-calling apps do not record exchanges on the device, but may generate a call log with the name of all the persons you have called. Network providers charge a fee for phone calls made using these apps.	■ Telegram ■ Line ■ WhatsApp ■ Signal ■ SMS ■ Voice Calling
Data Collection These tools allow workers to track their clients and report on their progress. The Microsoft Excel App does not always have automatic cloud back-up unless part a premium MS Office package. Google Sheets and Forms, on the other hand, enable collaboration and are stored securely online. They have a password-protected interface for program teams who will review the data collected. While QuickRes is a webapp, a shortcut can be created on the device's home screen for quick access to both the user-facing site and the back end. The worker controls client data that is highly secured and is not stored on the device.	■ DHIS II Tracker ■ MS Excel ■ Google Sheets ■ Google Forms ■ QuickRes
Added Security These apps will help keep your phone protected from online and unauthorized attacks. An antivirus app like Avast or Endpoint will block malware and cybercriminals while apps like Nova Launcher and App Hider can hide apps from unauthorized persons.	■ Endpoint ■ Avast ■ Nova Launcher ■ App Hider

2.4 Installing and Securing Apps

- Install apps that will be used for online outreach or virtual case management from app store.
- If a custom client management system is used for online outreach or case management, the systems administrator must install the relevant software.
- Do not 'allow' or 'enable' notifications when installing apps. Notifications already enabled on iOS devices can be switched off by going to Notifications in Settings. See which apps are using notifications and unselect them. On Android devices, go to the device's Settings, tap Apps and Notifications, then Notifications, and select the options you want as the device's defaults.
- Do not 'allow' or 'enable' Location when installing apps.
- Set up a "find my phone" service that will allow you to locate a missing or misplaced device using a web browser. For more on how to find your device, see this article for Android devices or this article for iOS devices. If the device is stolen, this can also help if the thief has not already wiped the device of its content or turned it off. If an MDM is used, it can help with removing the data from devices remotely.
- Create home screen shortcuts for regularly used program tools (e.g., token/link to Online Reservation App (ORA) or online client feedback form such as LINK). Use the steps below to create shortcuts:
    - **Android:** Launch device's browser (preferably Chrome) and open the web page you want to pin to your home screen. Tap the Menu button and tap Add to home screen. Rename the shortcut. Do this for specific tokens/URLs.
    - **iOS:** Launch the Safari browser on Apple's iOS and open the web page you want to add to your home screen. Tap the Share button on the browser's toolbar— the rectangle with an arrow pointing upward. It is on the bar at the top of the screen on an iPad, and on the bar at the bottom of the screen on an iPhone or iPod Touch. Tap the Add to home screen icon in the Share menu.
- Rename shortcuts to decoy webpages that may reveal the type of services offered by an organization. For example, instead of "HIV Services Registry" try "Shopping List". This can help prevent scrutiny by law enforcement, for example, if a worker is asked to provide their phone to an officer. Have internal consensus on the decoy names to prevent confusion.
- Dating apps like Grindr have a discreet app icon. You can change the icon by going to Profile>Settings>Security and then selecting the Discreet App Icon. This will allow outreach workers to decoy their Grindr app as another app such as a calculator or camera. For more on using a discreet app icon on Grindr, see this article. Apps like Nova Launcher and App Hider can be used to hide other apps in the same way on Android devices. Samsung devices also use Secure Folder, which can place certain apps and files behind a second layer of password protection using Samsung Knox security system that isolates and encrypts folder contents in the phone's storage.
- Creating home screen folders can also help hide apps from open view. This is usually performed by holding down the app icon until the user can drag it over another app to create a folder. For more on creating folders to store apps on Android devices, see this article.
- When going online with the device, check that websites' URL begins with HTTPS:// rather than HTTP:// or a lock icon in the address bar. This indicates a secured server, limiting the likelihood of data becoming compromised.

- Update installed apps every six months to benefit from new security features that may be introduced.
- Some apps, in addition to password protection, allow two-factor authentication ensuring they are only accessible by authorized personnel, even if someone knows a person's password.

2.5 Creating Worker Profiles

- Encourage the use of the organization's email addresses when setting up app stores and creating accounts for third-party apps used for online outreach and case management. A payment method is not typically required for setting up an app store. Payment may, however, be required to access premium features on dating apps like Grindr.
- Social media and dating apps will require a profile that includes:
    - **Display name** that considers the nature/culture of the platform. On dating apps, it is acceptable and recommended to use an alias. An outreach worker may put themselves at risk using their full name in spaces where most users are anonymous. Phrases such as "online outreach worker" or "your_link" are some professional examples. Outreach staff can decide to use their preferred names on social media platforms. Facebook may reject profiles that include fake or generic names such as John Smith; apps like Instagram and Twitter may allow creative use of display names.
    - **Bio** section that can be used to describe the services or support being offered by online outreach workers or the organization. It can also include web links and contact information for the organization. Eye-catching lines, such as "I am a Sexpert! Ask me anything about sexual and reproductive health" help grab attention and make the profile more appealing.
    - **Display picture** because users may not immediately trust a profile without an image. This may be different for dating apps since most people are anonymous, but on social media, an image is preferred. Try to use the organization's logo as the display picture where a personal image is not used. Outreach workers who are comfortable doing so may use their own images on social media but must first be walked through the possible risks of being identifiable (such as being contacted outside of work by clients, solicited sexually by clients, outed to friends or family as a worker in an HIV program, outed as a member of a key population). Those who choose not to use an identifiable image could use an image in which they could not be identified such as a profile shot with low lighting, a filtered photo, or a cartoon or avatar that protects their anonymity. Staff should confirm their choice of profile photo with their organization management to ensure it is professional, properly represents the organizational brand, and meets local staff security and privacy concerns.
- Consider making social media profiles private to individually add prospective clients. This will help with securing the profile user and list of followers from potentially harmful exposure. In addition to making the profile private on Facebook, ensure that the friends list is also private to persons who are not friends. See instructions here. On other social media platforms, like Twitter and Instagram, make the profile and posts private to prevent other users from seeing the list of followers.
- See online help tools provided by various platforms to set up and secure online profiles: Facebook; Twitter; Instagram.

2.6 Inventory

- Create an inventory of mobile devices. Document each device's model, product number, and other identifying features (e.g., the IMEI number found on the back of each device).
- Follow your organization's and/or donor's inventory guidelines, which may include assigning codes and labelling new devices and equipment.
- Prepare a contract that details how workers should use and protect devices used for online HIV outreach. Have staff sign the contract for devices that have been assigned to them. This contract should also include indemnities. The agreement, if properly written and enforced, will significantly reduce security risks.
- Hold devices in a secure area within the organization when not assigned or in use. This could be a password/code-protected safe, a cabinet with a lock and key or password, or a storage closet with lock and key or password. Ideally, the safe storage area should have charging capabilities. For example, lockers built into a wall can have plugs inside individual units. If a key is used, ensure that the key is kept securely, with access restricted to limited persons.
- Create a logbook/file/sheet for workers to sign for devices assigned to them or for devices that have left the facility.
- Have a clear policy on what workers should do if a device is stolen. For example, this may require reporting to the organization within 24 hours and filing a police report (notably, working with law enforcement will not be a secure option in some settings; this should be determined by the project based on the local context).

2.7 Maintenance

- Designate a worker/supervisor who will help with maintenance and inventory of mobile devices if your organization does not have IT personnel and an MDM is not in use. This person can use an Excel-based tracker to record notes on each device such as the date last checked, whether password was changed, and any other issues reported.
- Run regular software updates on each device. This is the best way to limit threats from malware and viruses.
- Have check-ins with each user to ensure devices are accounted for and are operating without issues. These should occur at least once per month.
- Plan and budget for device upgrades by monitoring new releases. Devices that become outdated may no longer support newer versions of various apps.
- Follow guidelines in 2.1 Setting Up Devices.
- Set up automatic back-up for Android and iOS devices to prevent data loss. Some messengers and apps that store data on the device itself will have options to back-up data periodically to their cloud (can be done manually or automatically). This is typically enabled in Settings of the app. However, general back-up for the device has to be done manually or set to automatically back up over a specified period of time.

2.8 Training

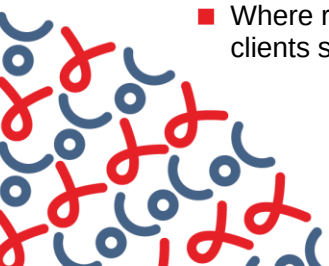
- Establish standard operating procedures (SOPs) that offer specific guidance on using mobile devices in online HIV outreach and case management. This may be in addition to a contract that staff already have that governs the general use and security of devices. The SOPs are for online outreach workers and case managers who use program tools for managing client cases, reporting service delivery, or collecting client feedback. See 3. Client Privacy and Data Protection and 4. Virtual Case Management to inform SOPs and training content.
- Use SOPs and other help tools to train staff to use devices for online HIV outreach and support them as SOPs are revised or updated. Management may also opt to have workers sign the SOPs, or each module within the SOPs, as an indication that they understand and will honor the guidelines.
- Enforce internal guidance regarding the use of organization resources. If use of mobile devices is not available, follow the guidelines in this document.
- Walk through the features of the devices and the expectations when using them with each worker.

2.9 Replacing Devices Not Lost or Stolen

- If you are still able to access the device you are replacing, be sure to back up all information recorded on it to your cloud storage. This is especially important for messengers like WhatsApp and Telegram so that chats are not entirely wiped.
- Once back-up has been completed, erase all information on the phone by performing a factory reset (see details under 2.10 Lost and Stolen Devices).
- If the device you are replacing cannot be powered on for a factory reset or is inaccessible, lock away that device in a secure storage area and do not reassign it to any worker. Do not take this device to a mobile phone technician or repair shop because as they try to repair the device, they may interface with sensitive client information or remove key features. Some data repair technicians could also install secret key login screens. For more on secret key login screens, see this article.
- If you decide to return a broken or damaged mobile device to a vendor covered by warranty, be sure to back up and delete all the information from the device. If it is not possible to delete the information, do not return it if any of the information could be used to identify either workers or beneficiaries.
- Follow guidelines in 2.1 Setting Up Devices.

2.10 Lost and Stolen Devices

- Render a device “lost” if within 24 hours you are unable to locate it on your person or within the facility. Recall the “find my” feature described in Section 2.4, which can be used to help locate a device that goes missing.
- Inform your network provider immediately if a device is stolen or lost. They will then block outgoing and incoming communications to the telephone number assigned to that device.
- Where relevant, staff should advise clients that the device was lost or stolen. For example, if clients should stop using a specific number because it is no longer in service.



- Follow these steps to deactivate access to apps installed on the lost or stolen device:
    - **WhatsApp:** Send an email to support@whatsapp.com with the phrase "Lost/Stolen: Please deactivate my account" in the body of the email and include the phone number in full international format.
    - **Facebook:** Log into Facebook on a different device. Go to Mobile Setting > Select Lost Your Phone?>Log Out on Phone (here). You should also change the password for your Facebook account.
    - **For other apps like Twitter, Instagram, and Google**: Access your account from a different device and change your password. You will be prompted to log out of all devices.
- Contact your local police to report devices that are stolen if it is safe for your project to do so. Follow guidelines in 1. Choosing Devices when acquiring a new device.
- Staff should also prepare a formal report for the organization that:
    - Includes their name, position, and the telephone number assigned to the device
    - Details the make and model of the lost device
    - Declares the point at which the device went missing and under what circumstances

2.11 Public Network Connections and Wi-Fi

- Turn off Bluetooth or Wi-Fi when they are not being used. Network data settings can remain constantly enabled.
- In the field, connect to mobile data and do not connect to public Wi-Fi. This can put devices and data at risk for malicious attacks.
- Do not use mobile devices used in online HIV outreach as a tethering device (hotspot) for other devices **not** used for HIV outreach.
- Be mindful of network spoofing where hackers set up fake access points—connections that look like Wi-Fi networks but are traps—in high-traffic public locations such as shops, libraries, and parks. Cybercriminals give the access points common names like “Free Library Wi-Fi” or “Coffeehouse” to encourage users to connect.[6]

2.12 Outreach Staff Using Devices Off-Site

- When devices are taken off site, they should be kept safe and not placed near water or heat.
- Tablets taken off site (in the case of mobile testing) should be kept in the custody of an assigned worker and returned to that person after collecting data. That person is also responsible for ensuring the safe return of the device to the facility.
- Do not leave devices in vehicles when not in use; they should be in the custody of a staff member or in the designated storage area.
- Do not leave devices out, even at your facility, unless supervised by a worker, e.g., when collecting routine quality improvement data.

- Devices stored at the facility must be locked away in a secured cabinet or drawer.
- At home, lock the device away in a safe place known only to you. Program teams may consider secure storage options for workers who keep devices at home.
- In public spaces, use headphones when listening to the phone so that the device is out of sight. Pay attention when people approach you on the street for directions, petitions, canvassing, and so on.
- Remember that someone could grab your phone from your hand. Make it hard to get to while you are using it, especially on public transportation or in a crowded space.
- If outreach workers are traveling in an area known for pickpockets, they should keep mobile phones in a phone pocket or otherwise tucked away.
- Do not give unlocked mobile phones to strangers to make phone calls. If a mobile phone is given to a client to make a call for any reason, that person should be closely monitored by an outreach worker.

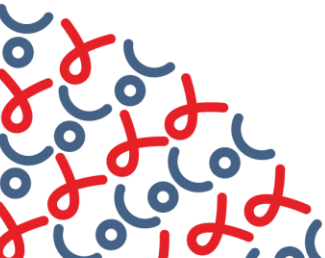
2.13 Site-Based Data Collection/Surveys

- When supporting clients to complete surveys such as LINK, take them to an area where it is quiet and as private as possible. Do not shout the questions.
- If a client wants to complete the survey on their own using a tablet device at the facility, be sure to give them privacy. Be on standby to offer any support the client may need.
- Ensure that after each survey has been completed, the submit button is selected and the screen is completely free of the survey responses before handing that device to another client or worker.
- When the tablet is not in use, keep it locked away or in the custody of a worker who is easily accessible and may not leave the facility.
- Ensure that tablets, like mobile devices, used to collect survey data are password protected and remain screen-locked when not in use.

Pro tips for virtual client support staff

- Outreach workers should ensure that the apps and operating systems on their devices are regularly updated. Staff should also report any issues found with devices immediately to prevent further issues.
- Never disable phone lock; if applicable, ensure that the device is set up to lock screen after 10 seconds of inactive use. For more information on setting screen lock on an Android device, see this web page.

- Staff should not click on links sent in messengers and emails from unknown or anonymous senders. These links could compromise the security of the device or the accounts being used to access the link.
- Where possible, staff should regularly log out of social media accounts and dating apps used in online outreach. This will prevent unauthorized access when a device is lost or stolen.
- Outreach workers should monitor battery and network usage, and SMS or call charges; compromised devices may have unusual usage of resources or charges.
- Check for suspicious behavior of device Settings: malicious apps can automatically turn on your GPS, Bluetooth, or network settings. If a device's overall performance is reduced or restarts frequently, then most probably the device is infected with a virus unless it is a hardware problem. Report this immediately.
- Workers should not be misleading in their work profiles or use work profiles to meet new friends or partners as this can diminish trust in your program's brand. Instead, they should use a private account for personal connections.
- Workers who use social media and dating apps for online outreach should consider the "culture" of the app and use avatars and logos as default images—especially in user-anonymous spaces.



3. Client Privacy and Data Protection

This section provides guidance and considerations regarding client privacy and protection of client data for staff providing virtual client support.

Important: Basics of client privacy and data protection

Programs should ensure the collection, use, and storage of clients' personal information is undertaken in such a way as to always protect clients' privacy. If not, organizations are at risk of:

- Illegally collecting and storing client information on mobile devices.
- Exposing clients' private information if asked by law enforcers to grant access to mobile devices used in online HIV outreach. (Note that such requests may be legal or illegal based on local laws; however, even in cases where the request is illegal, harm may come to an individual who does not comply with law enforcement requests, so it is preferable to limit the data that may be viewed).
- Bringing further harm to clients experiencing intimate partner violence at home.
- Outing clients as members of key populations and/or revealing their HIV status when staff share screenshot or chats and save contact information with identifying or compromising data.
- Sharing client information with unintended persons within the organization or those who see the screen in a public space.

3.1 Monitoring Local Laws

- Check for laws within your country that govern the use of personal or health care data or use of electronic devices to administer health care services. The Ministry of Health or local lobby groups may be able to help identify such laws or policies. The international law firm, DLA Piper has prepared a public-facing database of data protection laws around the world. The United Nations Conference on Trade and Development (UNCTAD) has also published a similar database.
- Create a list of all the applicable laws and share with staff. Staff should also be fully abreast of the current laws that govern sharing health care data while being aware that many countries laws regarding data privacy are nascent and/or missing specific components. The patchwork of laws, and/or limited enforcement of existing laws, can create a high risk environment for implementers trying to enforce security and privacy of data.
- Some countries may not have adequate laws to protect client data or online engagements. Stricter standards of client privacy and protection must be employed while obtaining, accessing, collecting, analyzing, or otherwise using data on key and vulnerable populations.

- Regularly monitor the press and official government releases for any new policies or laws that will affect online outreach. Make a note of such changes and advise outreach staff of the steps to be taken.

3.2 Protecting Conversations

- Always keep devices password-locked and stored in a lockable space when not in use. Close chat-enabled apps when not engaging clients.
- If you access apps from a desktop or laptop computer, ensure that you have completely logged out after each session. WhatsApp web is a common example.
- Encourage clients to shift to more secure and private platforms when conversations become more private and sensitive. Messengers such as WhatsApp, Telegram, and Signal include end-to-end encryption. For more on encrypted messenger apps, see this article.
- Do not take screenshots of conversations. If you must screenshot a chat for quality improvement, block out any identifying features like pictures and names. Note, however, that the 'markup' or 'drawing' capabilities in iOS devices are not intended for redaction and can be undone easily. See more on how such markups are removed here. When using iOS devices, it may be better to crop the screenshot to remove the names or images from the chat.
- If clients share private and compromising images for diagnoses, workers must delete these images from the camera roll. Outreach staff must advise clients against sharing images unless directly with a trained virtual clinician.
- Ensure that no one can see the details of a live conversation. Find a place where you are alone if you can.
- Do not forward conversations to anyone or yourself.
- Ensure that your clients are aware if you share devices with other members of your team.
- Organizations can install and enable an encryption app on tablets and smartphones. Encryption methods vary based on the device. Research your device's encryption capability. For more on built-in encryption for Android devices, read this article.
- For additional security when texting, disable notifications preview on the device. If you do not have notification preview disabled, then others can view text messages on the locked screen without authenticated or authorized access.
- Outreach staff must refrain from sharing their specific location or family name when conversing with clients and must advise clients to do the same.
- You may wish to delete the chat history with the client after you complete your session and advise clients to do the same. Alternatively, you can use disappearing or "self-destruct" messages for your support to clients that will be automatically deleted after a set time or after being viewed by the recipient. For more on apps with self-destructing messaging, read this article.

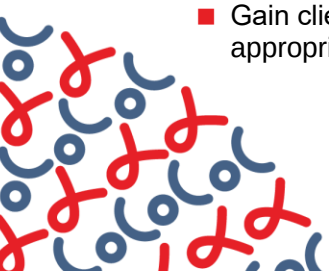
3.3 Saving Personal Information and User Preferences

- Do not save client's personal information, such as addresses, on a mobile device.

- Workers should not save their own personal information on mobile devices used for outreach. This may include address, banking information, or personal notes.
- For apps like WhatsApp, do not save a person's surname as part of their contact details. Save only their first name and first letter of surname, for example, Christopher E.
- If personal details are shared with you in a chat, record that detail off-line or in your secured online client tracker tool (e.g., QuickRes) and delete it from the chat. Advise the client that you have done so.
- Do not add compromising words such as "MSM," "Grindr," or "DL-Top" to client's contact information as this could make them a target for harassment if data is accessed by unauthorized persons.
- Depending on the types of services accessed by each user, an outreach worker or case manager may provide sensitive information with the user via mobile device; this may include test results or clinic appointment times (e.g., "We have your test results; please call XXX to access them." Or, "Your test result is positive; please schedule a follow-up appointment by calling XXX or clicking this link). The options for sharing such information should be dictated in organizational SOPs. The client should have the final decision on what is shared via mobile device and should be encouraged to consider issues such as shared ownership of devices, whether a partner or other family member may read messages shared electronically, and the emotional impact of receiving a test result without immediate counseling available.

3.4 Voice and Video Calling

- Ensure that you are in a private and quiet space when having a phone call with a client.
- Do not speak with clients on speaker phone, opt for a headset.
- Do not send pictures of yourself to a client as this is not essential for providing client support and may be interpreted as a personal advance/interest in the client. Additionally, these photos can be used by clients to stalk staff or report staff to authorities and put you at risk or facing undue hassle explaining your virtual client support role. If clients want to confirm who you are and your authenticity, ask to meet in person at your facility.
- If you must take a call at home, be sure to inform the client that you are taking the call from home. Only take the call if you can find a private place to talk.
- Do not have a video call with a client you have never met unless they were referred to you by another trusted organization.
- If a client requires to talk on video, first advise them that you are taking the call at your office and the audio may be louder than a standard phone call.
- When taking a video call at home, ensure that the background is clear of family members or distracting items. Stand or sit against a wall if possible.
- Do not take calls on public transportation.
- If you must defer a call, check that it was not urgent with a text message and schedule a time to speak later.
- Gain client consent before contacting the person by phone. For example, ask "Would it be appropriate for me to call you on this number? If so, at what times? Who should I ask for when I



call, and who should I say is calling if someone else picks up?" This can be especially important if the client is experiencing intimate partner violence or family abuse.

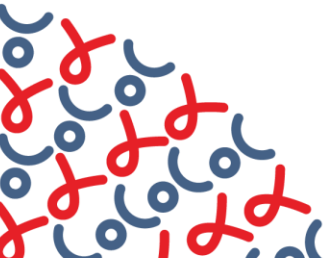
- Gain client consent before sharing their contact details with another team member or organization. If client consent is gained over the phone, ask that this be documented in an agreed-upon platform such as WhatsApp or Telegram, e.g., "Thanks for our call earlier, I want to confirm that you are okay with me sharing your contact information with our site nurse." The client must respond with an affirmative "yes" or "okay." If consent is not clear, workers must restate their request to gain clarity, e.g., "So just to be clear, are you fine with me sharing your number with our nurse? She may call or send you a message on WhatsApp."

3.5 Engaging Clients on Social Media and Dating Apps

- You may use social media and dating apps to meet new clients online. Once you have established a connection with your client, it is best to transition to a messenger app like Viber, WhatsApp, or Telegram for a more secure exchange of private and sensitive information.
- Be mindful of people who pretend to be someone else online. They are often called a "catfish." They usually have hidden intentions and can pose a threat to your safety.
- When joining a Facebook group as a representative of your organization, check whether it is a Secret or Closed group. Your behavior may be different in a setting where you do not know with whom you are interacting. If your program decides to create a group, make sure it is a closed or secret group. Closed groups can be seen by the public and visible in search, while secret groups cannot. If you create a closed group, the name, the members, and the description can be seen by the public—everything except the posts. Ensure this is known by group members and choose the group name carefully.
- When joining a closed or secret group as an outreach worker, write a message to the group owners explaining your role and why you would like to join. The owners can help provide you access and guidance on your messaging to members so you can avoid being banned or kicked out.
- When posting information on a public social media page, avoid sharing:
    - Images that show your face or faces of team members (even if they are in the background) unless you explicitly get their permission.
    - The physical address of a meeting or event, particularly those for populations that are stigmatized or criminalized. Advertising the location can put attendees at risk. Opt for asking clients to reach out to you for more details of upcoming events and meetings.
    - Your personal phone number and opt for sharing your work phone number or asking clients to reach out to you by starting a chat on your social media profile.
    - A personal account if you are the administrator of a page; make sure that your account is private.

Pro tips for virtual client support staff

- Outreach workers should be encouraged to educate their clients about the local legal environment, including letting them know what is safe and unsafe to share electronically. They should also know how to seek redress if laws, such as privacy laws, are broken.
- Workers should advise clients that they do not have to share identifying information such as surname and location. Clients may also be encouraged to delete the chats after each session if they so desire.
- Outreach workers should not take calls on public transportation or while walking in public.
- Workers making a phone call to share clinical information related to lab results or treatment, must start with pre-counseling. Ensure clients are made aware of all available options for support if their results are unfavorable before sharing information. Check in with clients about how they feel before and after sensitive information is shared with them and offer post-counseling and additional support. If possible, encourage clients who pass COVID-19 screening to visit the clinic to receive sensitive information and support. If not possible, periodically check in with clients and make plans to connect them to other forms of virtual and consistent support.



4. Virtual Case Management

This section provides guidance for staff providing virtual client support, tailored for clients in long-term care—such as those on antiretroviral treatment or pre-exposure prophylaxis (PrEP)—called virtual case management. Outreach workers and case managers may be using a client management system for tracking and support. Some systems have a security feature that protects client privacy and personal identifying information (for example, the QuickRes global online reservation and case management app developed by FHI 360).

Important: Basics of virtual case management

Virtual case management is concerned with online support provided to new and existing clients over time. This includes regular reminders, counseling and, sometimes, consultation. Some security risks of this approach include:

- Unintentionally outing clients to their partners or peers if proper verification is not performed.
- Saving client information without informed consent.

4.1 Creating Identifiers

- Outreach staff should communicate with clients about the importance of collecting identifying data such as mobile number, date of birth, age, and sex. These are some examples of data that can be used to identify client records and provide long-term support. If a client does not want this type of information documented, outreach staff should inform the client that their cases may be treated uniquely every time they access services. In such cases, the facility is unlikely to have and identify records or appointments where a case management tool like QuickRes is used.
- For clients who do not own a mobile phone and are reached through a friend or their partner, use an emoji to make that distinction and make a note in the contact's name: for example, Sean P 🚫. In such cases, staff should call and request to speak to that individual.
- If you are contacting someone who does not have their own device, ask them how the person calling should identify themselves to avoid causing problems for the client. For example, "Should I call and say that this is James calling to speak with Matthew or should I identify myself as a health care worker calling to speak with Matthew?"
- Encourage clients to use an alias or nickname when storing outreach workers' names or the organization's phone number: for example, instead of "Jamaica AIDS Support for Life," use "JASL."

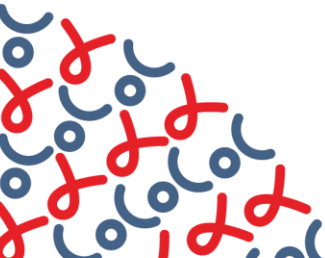
4.2 Verifying Client Identity

Ensuring you are speaking to the right person, whether communicating in person or virtually, can be challenging. This is particularly important for outreach staff or case managers who follow up with clients by phone before and after service access. Follow these steps to verify client identity:

- Upon first communication, you can assume you are talking to the person they are presenting themselves as and you will have to collect some basic information such as name, birth date, and other details to register them in your outreach tracker (or QuickRes).
- Ensure the client knows how this information will be used and where it will be stored. If they do not wish to provide specific information, such as birth date, allow them to skip these questions.
- In subsequent communications, you may perform an identity verification based on information submitted earlier.
- Develop a standard set of questions to determine client identity and use it every time you re-engage with the client by phone or other communication app.
- Some identification methods include:
    - Verifying client birth date and name
    - Verifying another unique code assigned to the client
    - Verifying client identity assumes that you have a file or tracker with client information that you can use to verify the client information (such as QuickRes).
- For example, see this guide on Health Insurance Portability and Accountability Act (HIPPA)-complaint patient identity verification methods.

4.3 Routine reminders

- Do not send SMS texts to mobile devices that the client has indicated they share with a friend or partner. When using client management systems with SMS feature (such as QuickRes), allow clients to opt out of receiving SMS.
- Encourage the use of an alias or nickname for clients to protect their identities.
- If supporting a client to make reservations on online booking platforms (such as QuickRes), ensure you read to them a summary of key points on that platform's data use and privacy policy so they are aware of what data may be collected, how it will be protected, and how it will be used/viewed by various staff members.
- When sending SMS, through QuickRes 'Bulk SMS' or from a mobile device, do not include any text that would reveal anything about the nature of health services being provided to the clients. Avoid messages like, "Your next HIV follow-up appointment is next week" or "Don't forget to pick up your ART tomorrow." Use neutral language like "Your medical appointment is next week," or "Your medication will be ready for pickup tomorrow."



References

[1] We Are Social Inc.[Internet]. Digital in 2020. New York: We Are Social Inc.; c2008-2021 [cited 25 April 2021]. Available from: https://wearesocial.com/digital-2020.

[2] ICTworks. [Internet]. 4 ways HIV programs can go online to mitigate COVID-19 impact. 2020 April 29 [cited 25 April 2021]. Available from: https://www.ictworks.org/hiv-programs-online-mitigate-covid-19/#.XulhpPlKguX.

[3] For instance, the Samsung Galaxy Tab A 10.1" WiFi+LTE available on the Samsung website.Available from: https://www.samsung.com/us/mobile/tablets/galaxy-tab-a/.

[4] Newman LH. WhatsApp has shared your data with Facebook for years, actually. San Francisco (CA): Wired Magazine; 2021 Jan 8. Available from: https://www.wired.com/story/whatsapp-facebook-data-share-notification/.

[5] Duffy Nick. Grindr disables location data over security loophole. London: PinkNews; 2014 Sept 6. Available from: https://www.pinknews.co.uk/2014/09/06/grindr-disables-location-data-over-security-loophole/.

[6] Kaspersky [Internet]. Top 7 mobile security threats in 2020. Moscow: Kaspersky; c2021 [accessed 26 April 2021]. Available from: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store.