Guidance on security measures for frontliners

Digital Security

Psychosocial security in our guide refers to ensuring the psychological and social well-being and safety of frontliners. The psychosocial security of frontliners is another priority that should be focused on, given the nature of their work and the different cases and stressors that they may be subjected to, all of which are further exacerbated in light of the recent COVID-19 pandemic. Their work, which focuses on human rights of PLHIV and key populations, service provision and follow-up care and support, often exposes frontliners to cases that are suffering from a number of violations, sometimes exposing them to compassion fatigue when they are affected by cases that they are following up on. The effort and dedication that frontliners work with often takes a toll on their emotional and mental health increasing their risks of stress, anxiety, depression, and even burnout, if not equipped with the proper coping skills and psycho-social support to mitigate these risks.

Measures to be taken to ensure digital security of frontliners

Frontliners

- **Protect your anonymity:**
  Do not give out real name or information related to personal address or location to someone that you do not know over the internet. Always use a pseudonym, especially when working on online awareness through dating apps, etc...

- **Ensure confidentiality:**
  Use end-to-end encrypted applications such as WhatsApp for calls, chats, and file sharing.

- **Separate work and personal accounts:**
  Try to secure, with your organization, a dedicated line for work related calls, as well as separate social media accounts, especially in light of COVID-19 - where there is more virtual outreach.

- **Password security:**
  Change your passwords frequently. Use different passwords for different accounts. This includes email, social media platform apps, and telephone passcodes.

- **Device protection:**
  Lock your computer and phone. Do not share them with others unless you trust them and you can monitor what they are doing.

- **Data protection:**
  Connect your phone to your online account (Google or iCloud) in order to be able to access it and erase all data remotely if it is lost or stolen. For android users, install “Find My Device” app and make sure that it is enabled along with option to allow remote lock and erase. For iPhone users, enable the "Find iPhone" app. Immediately login and erase all data if your phone is stolen.
  - Android: through “Find My Device” app on another phone or tablet, or through website: android.com/find
  - iPhone: through another iOS device or from a website: iCloud.com.

HIV Organizations

- **Digital security training:**
  Provide HIV frontliners with digital security trainings on a periodical basis.

- **Secure your organization’s online presence:**
  Ensure security and data protection of your organization’s website, social media platforms and email servers and communications through liaising with professional IT firms.

- **Data protection:**
  Install a remote wipe software on all laptops and tablets that may be used in the field or at the office. Check with your IT service provider for the most relevant software for your organization. Remotely access and erase all data from any stolen device.

Safety & Security definitions

Security relates to intentional harm such as acts of violence, aggression and criminal acts.

Safety relates to unintentional harm or accidents, events, or hazards.

The terms are used interchangeably throughout this guidance document.

The development of this document was funded via the USAID-supported LINKAGES project.