ENDING VIOLENCE
Association of BC

PRIVACY TIPS FOR ANTI-VIOLENCE ADVOCATES WORKING FROM HOME[1]

The Purpose of this June 2020 Bulletin

During the COVID pandemic, when physical/socialdistancing is required, many community-based advocates are working from home. In this moment, technology plays a vital role, ensuring that survivors in need can still access critical support services. Antiviolence workers may be accessing agency files remotely[2] or connecting with clients via online chat or video calls. Just as in pre-pandemic times, our priorities must include protecting the privacy and security of client personal information. This Bulletin sets out basic privacy tips to guide anti-violence advocates working outside the office. It is intended as a guide and is for general information only. It is not intended to be, and cannot be, relied upon as legal advice. Compliance with the law remains with each individual or organization.

General Principles

Keep it Clear[3]

Be open and clear with survivors about what you are doing with their personal information. (See below for what to tell them if you are using technological tools.) Tell them why you need the information, what you will do with it, and with whom you are going to share it. Inform the survivor about the communication device/platform you will use and about any technical requirements that need to be in place for them to engage.

Inform clients before you begin digital service delivery. Inform them about the security safeguards and risks related to using the tool. Let them know you cannot guarantee conversations will not be intercepted. Remember, if the survivor lives in a remote community, they may have

[1] This Bulletin draws heavily on the foundational work on internet security done as part of the U.S. National Network to End Domestic Violence's ***Safety Net Project*** and the BC Society of Transition House's ***Technology Safety Project***.
[2] In this Bulletin, working "remotely" means accessing office data management systems from a home office.
[3] These subheadings are adapted from ***Community groups and COVID-19: What you need to know about data protection***, a Blog by Ian Hulme of the UK Information Commissioner's Office.

limited access to high-speed internet. Offer low-tech options such as the use of a telephone.

Consider that the use of a certain technology may be a barrier for the survivor. Does the platform support language characters for the language you are using and/or does it allow for the participation of a translator? Does it allow for TTY or sign language interpretation? If possible, use platforms that can accommodate these needs or that maximize access. Ask yourself: Does the technology require the survivor to download an app or create an account? Consider working with your agency to create electronic handouts/e-bulletins or tip sheets for clients on how they can access online platforms you are using to provide service.

Keep it Safe

Let the survivor know that they are responsible for the security of their own device. Alert them to possible risks associated with the use of their device in a home environment or where the device is a shared device. Let them know where they might get help identifying any signs that an abuser might be using spyware to monitor or control social media accounts, text messages, and GPS location.[4] The Peace Geeks Blog cited here and in the references section includes key steps the survivor can take if they suspect their device is being monitored. Make sure you have some basic safety planning conversations at the front end.

Keep it Consensual

Once you have told the survivor the above, they can consent to the use of the tool. Consent can be in written form, electronically documented, or verbal.

Here are some tips:

- Obtain consent and document it before you start a remote connection. Ensure that the survivor has clear information about how their personal information will be collected, used, and, in rare circumstances, disclosed, by your agency, and alert them to possible risks associated with use of their device before obtaining consent.
- One approach is to go over, verbally, the consent form with the client.
- If the consent is verbal, you should document in your file that the consent was verbally obtained.

Keep it to a Minimum

- Collect, use, and keep just what you need to provide the service to the survivor.
- Check to see if you require approval before removing records from the office. Some agencies have determined that no paper files should go home because you can access the data remotely via a secure server.
- Only remove personal information from the office if it is necessary to carry out the job and include only the specific materials you need to deliver your part of the service.
- Take care in transporting information home. Do not leave records, a laptop or

[4] See: COVID Blog #5: ***A Survivor's Resource Guide on Tech Safety and Support – Combating Domestic Violence During and Beyond COVID-19.***

other devices in your personal vehicle or in the care of anyone else.

- If you do take files home, make sure they are kept in a secure place away from others living in the home.

Keep it Lawful

The *Personal Information Protection Act (PIPA)*[5] governs your collection, use, and disclosure of personal information. When handling personal information ask yourself the following:

- Would the survivor expect me to use their information in this way?
- Has the survivor given me clear and informed consent to collect, use or disclose their personal information?
- Is the survivor's (or other's) health or safety at risk if I don't use or disclose their personal information?

If the answer to any of these questions is yes, then you can collect, use or disclose the information.

- Make sure you are doing only what is necessary and appropriate to the task at hand. Under PIPA, your agency must demonstrate that you have reasonable security strategies in place e.g. firewalls; anti-virus software; anti-malware; passwords in place; and privacy policies that apply in your workplace.
- Avoid platforms with known privacy problems.
- If there is a breach of your technology, inform your supervisor or your agency's privacy officer.

Keep it Secure

You must look after the personal information you collect. Here are some basic guidelines:

1. Physical Safeguards

Create a separate private workspace

- Ensure private conversations will not be overheard.
- Ensure it can be locked so others cannot enter. If using a computer, position monitor(s) so someone entering the room cannot see it.

Lock it away when not in use

- When working from home, ensure that you have adequate security measures in place to keep personal information protected such as a locked cabinet or drawer.
- If paperwork is involved, lock it away in a cabinet or drawer when not using it.
- Lock away laptops, tablets, USB sticks.
- If a device containing personal information is lost or stolen, notify your supervisor or your agency's privacy officer as soon as possible to determine how to contain the breach and whom to notify about it.

[5] Note that in BC, most community-based anti-violence programs will be governed by ***PIPA***; however, there are some exceptions. In BC, public bodies such as government ministries are governed by the ***Freedom of Information and Protection of Privacy Act (FIPPA)***. Whether or not a program is governed by ***PIPA*** or ***FIPPA*** depends on the wording of the contract the program has with their funding ministry. If the contract wording suggests that program records are under the agency or program's custody or control, then ***PIPA*** applies. For more information on factors affecting who has custody or control, see Ruebsaat (2006); or ***Community Coordination for Women's Safety Backgrounder: Critical Privacy Provisions Which Impact Information Sharing in Woman Abuse Cases*** (CCWS 2013)

2. Technical Safeguards

You want to protect against interception of the transmission e.g. a hacker gets into the call/transmission or an abuser is monitoring the device being used for the transmission. End-to-end encryption is the gold standard and recommended for interactions that involve the sharing of sensitive personal information.[6]

Privacy Protection Strategies

- Password-protect the device you use for mobile or online connection.
- If possible, use agency-owned devices and create work accounts for the sole purpose of communicating with clients.
- If you are not working remotely, with your information stored in your agency's server, back up your information/records until you return them to the office or until they are securely stored on the agency's database.
- Make sure passphrases or passwords are unique; use different passwords for each account. Use strong passwords e.g. use three random words together as a password: e.g. golflawntree.
- If using portable storage devices (such as a USB stick or portable hard drive), ensure they are password protected and encrypted.

- Keep software up to date. Make sure to install the latest updates.
- Log off/shut down laptop/computer when not in use -- make sure auto logoff is set for a short period. Note that log off/shut down is not the same thing as screen saver function.
- If you need to share data, choose a secure messaging app or online document sharing system or Virtual Private Network (VPN). Check to see if your agency has a recommended system. Ideally, information stored on the database or server will not be stored on the cloud.[7]
- Check the privacy and security settings/policies with your agency and/or with the vendor; ask the vendor if they sell client information; if yes, then this is a red flag. If possible, adjust the privacy and security settings to suit your agency or program needs.

Be Aware of the Risks

The section below outlines some of the privacy and security risks associated with text and instant messaging, email, and video-based communications and also sets out some strategies you can use to minimize the potential risks.

Risks Associated with Text and Instant Messaging

- Impersonation or interception.

[6] Simply put, end-to-end encryption means that only individuals who are parties to the communication can access the contents of that communication. The vendor or company selling the platform or technology being used cannot access or share the contents of the communication.

[7] Be aware that your funding contract may not permit storage of client personal information in the U.S. Best practice is to check that the system you are using stores data in Canada.

- Default settings of the vendor may allow for the collection, recording, storage, and selling of personal information.
- SMS texts that cannot be encrypted (only web chats can).
- Platforms that require participant to create an account that involves the vendor collecting personal information; (some platforms collect participant data and some don't; vendor collects this when client needs to download an app or program before they begin).

Strategies that can limit the risk

- Offer client additional ways to communicate that may be more secure, like web chat.
- Delete history after the communication is finished and suggest to your client that they do the same.
- Don't save client or participant names in your contacts.
- If possible, use agency-owned devices and create agency accounts.
- Turn off default settings if they allow chat messages to be saved, recorded or copied.
- Don't automatically back up text chats to cloud accounts or in Google Drive or a shared calendar. (These text messages and the history of the apps used and downloaded can potentially be accessed by others with the same cloud account.)
- Ask client at the outset: Does the abuser have access to the client's cloud account and any relevant passwords?; suggest the client check their device's set-up; can they set up their own cloud account?
- Find out if you can customize some of the privacy settings to disable certain functions as some options can increase safety risks; for example, can you disable the automatic record function?

Risks Associated with Email

- Most email is not encrypted and can be easily intercepted.
- Emails may be synced across devices.
- Several steps involved to fully delete emails.

Strategies that can limit the risk

- Avoid using email to transmit sensitive personal information.
- If you must use email, consider password-protecting documents and share passwords via a different channel e.g. phone.
- Don't click on unfamiliar attachments or links in an email. Spot suspicious emails. Watch for phishing.[8]
- Delete email and previous thread when you reply so if the abuser gains access the full history is not accessible. If you need to retain the info, print out the emails, then delete the digital version.
- Delete emails and then clear them out from their deleted folder/ delete box or trash folder on a regular basis; encourage client to do the same.

[8] Phishing is a tactic that scammers use to try and trick their target into giving away confidential information. The most common form is email attacks such as a message that appears to be from your bank and requires you to click a link to resolve an apparent crisis with your account or an email seemingly from a close family member pleading with you to send money to resolve a travel emergency, again, involving clicking on a link. You can also be "phished" via text messages, phone calls, instant messaging, and even social media. For more information, see Lookinglass Threat Intelligence Blog: ***What is Phishing and How to Avoid Phishing Scams*** at: https://www.lookingglasscyber.com/blog/threat-reports/phishing/what-is-phishing/?/

- Use work email accounts rather than personal ones for work-related emails containing personal information.
- Ensure you are sending the email to the correct recipient.
- Have a statement as part of your standard email signature box that automatically appears at the end of every email indicating that the info in the email is private and for the intended recipient only and that if it goes to the wrong recipient, they should delete it.

Risks Associated with Video-based Communications

There are advantages to using video-based platforms: the connection is more personal and may be more effective with younger clients or with those who have written literacy challenges. Also, with such systems there is a decreased risk of impersonation. Still, video-based communications share many of the risks outlined above with respect to chat or text messaging and email platforms.

As with other virtual platforms, not all video-based platforms are end-to-end encrypted. Some platforms share personal info between social media sign-ins, e.g. Google and Facebook; some allow you to sign in using your Facebook or Google account. This is not good from a privacy perspective.

Strategies to limit the risk

- If you go with this type of vendor, advise client not to sign in to the video platform through their social media account or Google account as this gives both vendors access to the info on the opposite platform;
- Advise client that to manage a poor internet connection they can use a combo of web for video and phone for audio so phone chat can continue if internet interrupted; develop a plan of action if client has to leave the call abruptly.

Keep a Record of What You Have Done

Keep a record of any decisions you make that involve the collection, use, and disclosure of personal information. At the time of their interview, make sure you keep notes of what you have done and why; make more detailed notes/records as soon as possible.

Return Your Records

Go to the office at regular intervals to return any files that you may have used while working from home. Check with your office as to what the protocol is with this in terms of how frequently and when.

For those who are unable to return to the office regularly due to being in the vulnerable population with respect to COVID, or living with someone in the vulnerable population (i.e. elderly, immune-compromised individuals) the office should make arrangements to have the records picked up by another employee or sent by secure courier.

Upon returning to the office, return any pre-existing physical records you used while working from home or created/generated while working at home, to their appropriate storage place as soon as possible and destroy any copies once you have done this.

For digital records, transfer the files to the appropriate agency database. Delete any digital records from any devices you used in your home office.

Getting Started on Working from Home: A Recap

- Check your surroundings; best practice is set up a private work space.
- Check your technology; have security systems in place before you get started.
- Use devices and platforms supplied by your agency if possible; if not, consider using a landline as your phone. This offers the least risk of interception.
- If you are using a home laptop or desktop, avoid storing data or personal information on that device as it might be used by a stalker to find out where you live.
- If possible, your agency should arrange access to the agency database or server remotely to enable storage of the necessary personal information there.
- Check that you have given the survivor notice of the tool you are planning to use to assist in the delivery of services.
- Get verbal consent for information collection, use, and disclosure. Keep a written record of the verbal consent.
- If using a computer application to connect by audio and video, make sure the application has end-to-end encryption and that there is no recording of the interviews as a standard practice by the vendor. (You may need to adapt the standard privacy settings to avoid the vendor recording the interaction.) It is also helpful to use the "waitingroom" setting if the app has one. This way no one can join the meeting without being vetted and given permission by you first.

For Further Information

For further information or to obtain additional privacy resources, please contact CCWS at ccws@endingviolence.org.

Additional Resources

British Columbia Association of Clinical Counsellors. (March 16, 2020). ***Remote counselling and privacy law***. Available for members at https://bc-counsellors.org/

British Columbia Association of Clinical Counsellors. (March 16, 2020). ***How do I choose a remote counselling platform?*** Available for members at https://bc-counsellors.org/

British Columbia Society of Transition Houses, Technology Safety Project. (2020). ***Digital services toolkit***. Retrieved April 23, 2020 from https://bcsth.ca/digitalservices/

British Columbia Society of Transition Houses, Technology Safety Project. (2020). ***BCSTH PEACE Program template: informed consent for digital support services***. Retrieved May 27, 2020 from https://bcsth.ca/wp-content/uploads/2020/05/BCSTHPEACE-Program-Informed-Consent-for-Digital-Support-Services-Final-May-12-2020.pdf

Information Commissioner's Office. (2020). ***Blog: Community groups and COVID-19: what you need to know about data protection***. Retrieved April 24, 2020 from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/communitygroups-and-covid-19/

Information and Privacy Commissioner of Ontario. (March 16, 2020). ***Impact of COVID-19.*** Retrieved April 24, 2020 from https://www.ipc.on.ca/newsrelease/ipc-closure-duringcovid-19-outbreak/

National Network to End Domestic Violence, Safety Net Project. (2020). ***Technology safety: using technology to communicate with survivors during a public health crisis***. Retrieved April 24, 2020 from https://www.techsafety.org/digital-services-during-publichealth-crises

National Network to End Domestic Violence, Safety Net Project. (2020). ***Technology safety: how to operate as a remote workplace during a public health crisis***. Retrieved April 24, 2020 from https://www.techsafety.org/remote-work-public-health-crisis

Office of the Information and Privacy Commissioner of Alberta (April 2020). ***Managing records when transitioning from work to home***. Retrieved April 24, 2020 from https://www.oipc.ab.ca/resources/managing-records-when-transitioning-from-work-tohome-advisory.aspx

Office of the Information and Privacy Commissioner for British Columbia. (January 2015). ***Protecting personal information away from the office***. Retrieved April 23, 2020 from https://www.oipc.bc.ca/guidance-documents/1447

Office of the Information and Privacy Commissioner and Auditor General of British Columbia. (October 2016). ***Mobile devices: tips for security and privacy.*** Retrieved April 23, 2020 from https://www.oipc.bc.ca/guidance-documents/1994

Office of the Information and Privacy Commissioner for British Columbia. (September 2019). ***Disclosure of personal information of individuals in a crisis***. Retrieved April 23, 2020 from https://www.oipc.bc.ca/guidance-documents/2336

Office of the Information and Privacy Commissioner for British Columbia. (March 17, 2020). ***Tips for public bodies and organizations setting up remote workspaces***. Retrieved April 23, 2020 from https://www.oipc.bc.ca/guidance-documents/2398

Ogorek, G. and Perry, M. (October 4, 2016). ***Lookingglass Threat Intelligence Blog: What is phishing and how to avoid phishing scams*** at: https://www.lookingglasscyber.com/blog/threat- reports/phishing/what-is-phishing/?/

Peace Geeks. (May 3, 2020). ***COVID Blog #5: A survivor's resource guide on tech safety and support – combating domestic violence during and beyond COVID-19***. Retrieved May 14, 2020 from https://peacegeeks.org/news/covid-blog-5-survivor's-resource-guide-tech-safety-andsupport-—-combating-domestic-violence

Ruebsaat, G. (2006). Records management guidelines: ***Protecting privacy for survivors of violence (3rd ed.)***. Retrieved June 8, 2020 from http://endingviolence.org/files/uploads/RMGapril2006.pdf

Ruebsaat, G. (2013). ***Critical privacy provisions which impact information sharing in woman abuse cases.*** Retrieved June 8, 2020 from http://endingviolence.org/wpcontent/ uploads/2014/11/CCWS-Privacy- Provisions-for-ICATs_Nov_20_2014.pdf