Protecting Survivor Privacy When Working From Home: A Guide for OVW-Funded Victim Service Providers[1]

We know that many agencies are implementing work-from-home policies virtually overnight. We are all facing new challenges in this time of a national health crisis. The Victim Rights Law Center's Privacy Team created this guide to help you navigate some of the logistics of working from home on such short notice. It is designed to help organizations implement best practices regarding privacy and confidentiality of victim information and comply with our obligations as OVW victim service providers.

Privacy is a fact-specific, case-by-case consideration. Inevitably there will be situations not anticipated below. Do your best and be mindful of privacy at all times. When in doubt, feel free reach out to your Privacy TA provider for guidance. You can reach the VRLC Privacy Team at: TA@victimrights.org.

All OVW-funded victim service providers (VSPs) are subject to VAWA's confidentiality requirements. VAWA states that a VSP "may not disclose, reveal, or release personally identifying information or individual information collected in connection with services requested, utilized, or denied through grantees' and subgrantees' programs, regardless of whether the information has been encoded, encrypted, hashed, or otherwise protected." 34 USC § 12291(b)(2).

"Personally identifying information," or PII, is information that directly or indirectly identifies a person. It may be someone's name, address, other contact information, or social security number. PII can also include someone's race, birth date, number of children or other identifying data. VSPs must protect the confidentiality of anyone who sought, received, or was denied services – this obligation is not limited to just the survivors[2] that you serve.

[1] This document is current as of March 31, 2020

[2] In this document, we use the term "survivor" to refer to anyone who is covered by OVW's confidentiality requirements—i.e., anyone who sought, received, or was denied services.

Workspace

Do not engage in any work-related tasks involving a survivor's PII where there is any possibility of a privacy breach.

At home, work in a space that provides privacy for the phone, computer, and any documents you're working with or conversations you're having (i.e., where no one else can view your screen, see your files, or hear your conversation if it involves PII).

Do not leave documents that contain PII in plain view or where they can be easily found by others, even if you are stepping away for "just a minute." This includes survivor-related paperwork such as files and forms, envelopes with a survivor's name and/or address, a survivor's phone number, notes from a phone call with a survivor, a name or number jotted down from a phone message, etc. To promote survivor confidentiality, as much as possible, work at home should be done from digital files stored on your organization's equipment that no one in your home can access rather than from hard copy files.

You will also need to dispose of information with PII securely. See the section on shredding below for more detail on how to dispose of survivor-related PII.

Communicating with, for, and about Survivors

While working remotely, you likely communicate with survivors in many different ways: by mail, phone, text, email, and perhaps videoconference. Each mode presents distinct risks and opportunities to protect survivor privacy.

Mail

If you are mailing documents to a survivor, the envelope or package should not be left sitting out with the name and/or address visible. If possible, do not leave correspondence with PII in your mailbox to be collected and sent by the letter carrier. Mail it yourself at the post office or a post office drop box. (If email is safe and accessible to the survivor, consider that as an alternative.)

Computers

For security reasons, if possible, any work involving survivors' PII should only be done on agency-owned equipment.

Email

Talk with survivors about the safety, security, and privacy implications of communicating by email. Be sure you have informed consent before you email with a survivor.

If your work email is set to alert you with a pop-up on your screen when a new email arrives, assess whether this presents privacy issues for your work from home. (See more on "computer screens" below.)

Remind the survivor to sign out of their email on any computer others can access. This is especially important if you are exchanging personal, confidential, or privileged information with the survivor.

Phone

Have phone conversations in private and confidential locations. Be mindful of both your and the survivor's location. If you have confidentiality or privilege, make sure survivors' communications with you continue to meet the requirements for a "confidential" communication under the law in your and their jurisdiction(s).

If you use a baby monitor take care that, if it's on, someone cannot hear your phone (or videoconference) conversation through the receiver or other means.

If calls will be made to or from a cellphone, it must be password protected. You should tell to your supervisor immediately if a cellphone with PII is lost or stolen. Organizations should have a policy that requires staff to make such a report as soon as someone discovers the loss or theft.

When deciding what phone you will use to make or receive calls from survivors (e.g., cell versus landline), pay attention to what information pops up on your phone's home screen when you receive a call. The caller's name or phone number may appear regardless of whether the call is made directly to your phone or forwarded to you from a work phone through an app. A survivor's name and/or phone number may appear on the home screen even when all notifications are turned to "off." If you cannot disable this function, you should have policies or protocols for how privacy will be protected when the phone is not in use or in your or another staff person's possession. Always be mindful of where your phone is and who can see the screen when a call comes in.

Consider the caller ID issue when you place a phone call. Caller ID works automatically with almost every phone service provider. Sometimes you can control this function by arranging for caller I.D. blocking your outgoing telephone number through your provider or the app. You may also be able to block your ID on a call-by-call basis by dialing *67 before you dial the outgoing number. The *67 code may not work with 800 numbers, though.

Privacy screens enhance, but are not a replacement for, the cellphone privacy practices and policies set out in this document. Consider using a privacy screen for your cell phone. They look like this:

Also be mindful of what information will be captured by the phone(s) in a call log. The call history (calls made, calls missed, etc.) may also automatically be saved in your personal cell phone log even if the calls were made or received through an app. If someone other than you or another staff person has access to your phone and you cannot disable this function, best practice is to delete the history for any calls made to or received from a survivor. (Survivors' telephone numbers are very likely to be PII.) Remember to check the voicemail log on a personal cell phone as personal information appears there as well.

If your work phone service is provided through Voice Over Internet Protocol or VOIP, and you have a desk phone at the office, you might be able to plug it into a data port at home and have it work just like it does at work. A few things to consider if you do this:

1. Make sure the phone is located where it has the privacy required.
2. Tape a piece of paper over the phone screen when the phone is plugged in to cover any caller's name or number, especially if the phone is going to be left out where anyone who is not a program staff member or volunteer can see the screen.
3. You may be able to set the phone to ring only during your designated work hours. This enhances privacy because callers' names and phone numbers do not appear on the screen when the phone is on Do Not Disturb. (It also helps with boundary setting during non-work hours!)

Phone bill: If you are using a personal cell phone for work and a friend or family member has access to your cell phone bill, be sure you know what information appears on your personal phone bill. For example, some phone bills list the phone numbers dialed, callers' phone numbers, and/or the phone number for anyone you texted or who texted you. If the phone bill is paid or can be accessed by someone who is not part of

your victim services program, you will need to ensure that your reimbursement, accounting, and auditing practices all protect survivors' personally identifying information. You may need to redact information from your phone bill before you submit it for reimbursement or arrange with your phone service provider to omit caller information from your bill. Know that not every provider offers this option. (If you are redacting the caller information from a personal phone bill you're submitting to someone outside your program for reimbursement, you may need to submit a companion statement or cover letter affirming that the calls were to - or from - survivors on the dates indicated.)

Remember, if you work for a domestic violence, sexual assault, dating violence, stalking and/or human trafficking program that is part of a multi-service agency, organization, or tribe, VAWA regulations state that you may not share any PII – including phone numbers on a phone bill – with individuals outside your victim services program without written and informed consent.

Video Conference

Videoconferencing presents significant opportunities and privacy risks. As an OVW grantee or sub-grantee, you have greater privacy obligations when communicating with or about people coming to you for services than you do when communicating with other staff members (including volunteers), or partner organizations, for example, on matters that do not contain any PII.

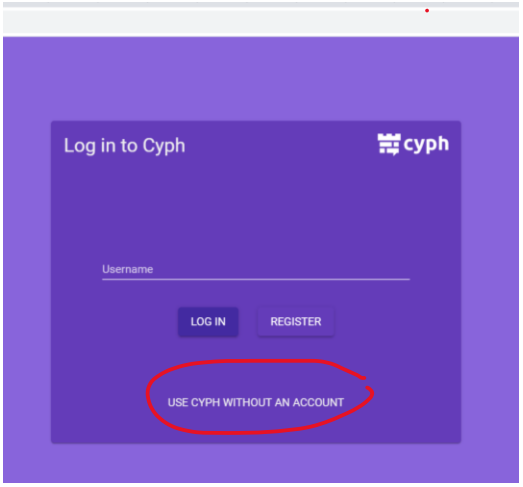
There are quite a few videoconferencing platforms available and you need to scrutinize each one before deciding to use it. You should get a survivor's informed consent to use any platform after discussing its privacy risks and protections. For more information about different platforms and the corresponding security, ease of use, whether they automatically record calls or keep a record, etc. see NNEDV's resource: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5e7e62a25ed80a4219adad77/1585341091261/NNEDV_Communication+Tools_Handout.pdf

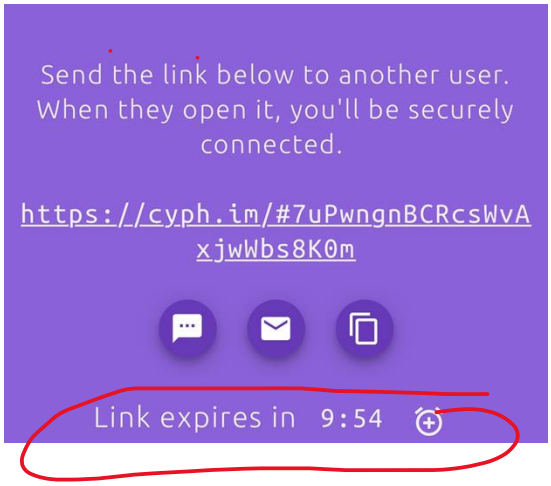
- Before you begin a videoconference with a survivor, make sure they are in a safe and confidential setting, and that it's still a good time for the two of you to meet "in person."
- If the survivor is video calling you from a location where someone might interrupt, discuss in advance what the "cover story" is for the video call.
- Remember that video conferences have audio too! Use headphones if others share your space, as this minimizes the likelihood that the person with whom you're videoconferencing will be overheard.
- Keep in mind that anyone on your end can still hear your part of the conversation, even if you're using headphones.

- Remember that VAWA and VOCA are more privacy-protective than HIPAA, so a HIPAA-compliant program does not necessarily meet VAWA and VOCA privacy requirements.

For survivors concerned they may be stalked by the perpetrator, there are free videoconferencing programs that do not require a user to download an app. Instead, you send the survivor a link that they click on to launch the session. Two such programs are Cyph and Doxyme. There are a number of others (see NNEDV resource linked above). VRLC does not endorse any one program. Those referenced here are cited just as examples, and should not be viewed as recommendations.

Cyph: Cyph.app is a free service that has the benefit of verifying the integrity of the application to ensure it hasn't been tampered with since it was installed. It asks for a user name and login, but you can also use it without registering for an account; click on the bottom where it says, "Use Cyph without an account."





You then send the other user a link to access the service; they must accept within 10 minutes or the link expires. (You can always click back in and get another link to send.) Note: Connecting through Cyph video uses a peer-to-peer connection, so you'll be connecting directly to the other party instead of going through Cyph's servers.

Doxy.me: Doxy.me is another free program. It is used most commonly by healthcare providers and psychotherapists. Like Cyph, you launch the session by sending the other person a link to use.

Microsoft Teams may be easy to use for anyone with a Microsoft account, but the risk of chats or communications being stored may present safety risks for survivors.

Similarly, **FaceTime** is very user friendly for survivors and providers with iPhones but deleting the call history requires several steps to eliminate the safety risks.

- **Note**: You and the survivors you work with may be required to participate in videoconferences set up by third parties such as courts, schools, or colleges. You may not be able to control what platform is used.

If you and the survivor are in different locations, and will be appearing by videoconference with other parties, establish a plan for how you and the survivor will communicate privately during the hearing. Whatever methods you plan to use, practice both them and the videoconferencing in advance of the appearance. Be sure to discuss how to use the "mute" function or go off-screen while remaining on the call (if permissible).

- Protect your own privacy. Be mindful that the person on the other end can see what's behind or around you. Take care that you're not inadvertently sharing information about yourself that you prefer to keep private.

<u>Computer Screens</u>

- Pay attention to what others can see if they walk by your screen or monitor, or if you walk away from it. Don't walk away from a computer with documents with PII left open on the screen.
- Consider whether to use a monitor privacy screen. It looks something like this:

- Note: A privacy screen helps if someone is looking at your screen from the side/at an angle. They provide little to no privacy is someone is directly behind you looking at your screen.
- Set your computer to timeout if you are away. (Go to Settings, Computer Settings, Power.) That way if you step away from your computer for a couple of minutes, and become distracted, your computer will timeout and require you to sign-in again to unlock it. (All Programs, PC Settings, Personalization, Screen Time Out Settings.)

Physical Files / Physical Documents

1. Transporting physical documents:
    - A survivor's file, folder, envelope, or other physical item should never leave the office or your home with the survivor name or any other PII visible. Such items must be transported in a bag, box, or envelope so that PII cannot be seen by others, and to ensure the item doesn't fall out accidentally.
    - Never leave anything with a survivor's PII in your car (if you're not in the car) or anywhere other than a private location not likely to be accessed inadvertently by others. Locked cars and car trunks are notoriously insecure; documents with PII should never be stored there.
    - When you take a break, are done for the day, or otherwise are not actively working with the documents that contain PII, secure the documents and ensure they're not accessible to others.
2. If you are working from home in a private office, and survivors' related PII is in use, any time you are not in the room or when you are done for the day the door should be locked or the files put away and not accessible to others.
3. Always close your laptop lid or turn off your monitor if you are stepping away from your computer.
4. Password protect all devices.

In-person Meetings While Working Remotely

Establish a protocol if an in-person meeting must take place. Criteria for an in-person meeting with a survivor should include whether you will be meeting at a location where confidentiality is preserved, whether the proposed meeting location presents a risk of inadvertently disclosing that you are serving a particular survivor, whether you have a VAWA-compliant signed release of information allowing you to identify the survivor at the alternate location if this is required to gain access or connect with the survivor, etc.

Scanning

For security reasons, we recommend you only scan documents that contain survivor-related PII to computers owned by your program. (Do not scan survivor-related documents to a personal computer.) Do not scan survivors' documents with PII at a commercial copy company.

Photocopying and Printing

Don't scan, photocopy, or fax documents containing survivor-related PII at a business (e.g., Kinkos or Fed-Ex, your friend's company). Have a plan in place for an unanticipated emergency requiring you to photocopy or print documents at a business.

If you are printing or photocopying at home, take extra care to ensure that you do not leave any confidential documents with PII on your copier or printer.

Tip: If you are working on a draft document consider using an alias or insert "XXX" instead of the survivor's name and omit any PII until you need to print the final copy. You can then do a universal "search and replace" before you print.

Destroying Documents with PII

If you have a home shredder you could use it for work documents. Make sure any documents are shredded completely before turning off the shredder. Documents with PII or other confidential information should never be recycled or thrown in the garbage unless they are shredded.

Other options may include securing the documents in a locked drawer, closet, or file cabinet (to which no else has the key) or transporting them back to your office (in a safe and secure manner, as discussed above) when they can be disposed of securely, or burning them (depending where you live, the weather, safety, etc.)

Try to be judicious in printing documents with PII at home to minimize the amount of paperwork that will need to be disposed of confidentially.

Securing Releases of Information (ROIs)

You are required to meet your VAWA and VOCA confidentiality obligations wherever you work. You may only reveal personally identifying information about someone who sought, received, or was denied services if you: (a) have a signed, written, specific and narrowly crafted, release of information that was executed with informed consent and is valid for a reasonable length of time; (b) a statutory mandate; or (c) a court mandate.

For a release to be "informed," you and the survivor must discuss why the survivor might want you (or a third party) to release information that is personally identifying, agree on what information will be released to whom, and record this agreement in writing.

Getting the written release safely signed and returned, while ensuring it was executed with informed consent, can be challenging when you are not meeting with survivors in person. Electronic signatures that are not a survivor's actual signature are not VAWA compliant. You may need to be creative in how you arrange to have the ROI signed. Some ideas include:

- You can mail or email the survivor a blank ROI for their signature (after confirming it's safe to do so), and then schedule a time discuss what to fill in. The survivor can sign the release and send it back to you. You could include a self-addressed stamped envelope with the release if you mail it.

- Another option is to discuss the terms of the release in advance and send the survivor a completed release that reflects this agreement for them to sign. If you send a completed form in the mail, it's best to put a blank piece of paper around the ROI to enhance privacy, in case the envelope is torn in transit.
- You can ask a survivor to take a photo of a signed ROI and email or scan it to you. As always, the survivor should only do this if you've discussed the privacy and safety considerations of this approach. For example, iPhones store photos even after they've been deleted for 30 days in a "deleted items" album, sent emails and attachments live in the "sent" folder, etc.
- If you are meeting with the survivor by videoconference, you can send them the blank ROI, discuss and agree upon what it should say, and have the survivor sign the document while you are both on video. They can then return the signed ROI to you by mail, email, etc.

Other

It is best not to not use Google Translate or Google Interpreter for documents or conversations that contain PII. Google automatically captures the content to have their staff review the accuracy of their artificial intelligence (AI) at work.

If you do inadvertently breach the PII of someone who sought, received, or was denied federally funded services, or if a breach is imminent, you must inform your funder within 24 hours from when you learn of the actual or imminent breach. So, if you lose a phone that has work-related content, your work laptop is lost or stolen, your email gets hacked, you lose a document or file with PII, you leave documents with PII sitting out and someone outside of your program might have seen them, or you otherwise have a breach event, follow your program's data breach policy.

Finally, know that you are not in this alone! The VRLC's Privacy Team is here to help. These are extraordinary times and we're all doing our very best to adapt as quickly as we can. Don't hesitate to reach out for guidance, discussion, or just because you need a friendly privacy consult. We're here for you!

You can reach the VRLC Privacy Team at: TA@victimrights.org.

 This project was supported by grant number 2015-TA-AX-KO25 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, and conclusions expressed are those of the author(s) and do not necessarily represent the views of the U.S. Department of Justice.