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

While some organizations had staff working remotely pre-pandemic, many others implemented work-from-home policies virtually overnight. The Victim Rights Law Center's Privacy Team created this guide to help you navigate some of the logistics of working from home. 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. The guide addresses everything from transporting files home, use of personal cell phones (and caller ID), scanning, printing, document destruction, videoconferencing, and more.

Privacy is a fact-specific, case-by-case consideration. Inevitably there will be situations not anticipated below. Do your best to be mindful of survivor[2] privacy at all times and know that you don't have to navigate this alone. You can reach out to the VRLC Privacy Team anytime. Email us at TA@victimrights.org or call us at 503-274-5477 x 1 and x 2. We're here to help!

All OVW-funded victim service providers (VSPs) are subject to VAWA's confidentiality requirements, which have a purpose "to ensure the safety of adult, youth, and child victims" and their families. VAWA states that, without a statutory or court mandate, or the survivor's informed, written, signed, and reasonably time-limited consent, 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." See 34 USC § 12291(b)(2) and 28 CFR 90.4.

"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

[1] This document is current as of May 10, 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.

sought, received, or was denied services – this obligation is not limited to just the survivors that you serve.

Workspace

Do not do 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 and 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.

Physical files and 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 should be transported in a bag, box, or envelope so that PII cannot be seen by others, and to ensure documents don't fall out accidentally.
    - Never leave anything with a survivor's PII in your car (if you're not in the car). Locked cars and car trunks are notoriously insecure; documents with PII should never be left or stored there.
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. No work device should be without a password.

Communicating with, for, and about survivors

While working remotely, you may be communicating with or about survivors in many different formats: by mail, email, phone, text, instant messaging, and/or videoconference. Each 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 to others. Do not leave correspondence with PII in your mailbox to be collected and sent by the letter carrier if anyone else in your household has access to the outgoing mail. 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 and computer screens

For security reasons, if possible, any work involving survivors' PII should only be done on agency-owned equipment. It is best if the computer can be wiped remotely in the event it is lost or stolen. The computer should be password protected. Take care not to leave the password in an obvious place (e.g., under the keyboard) or use a password your family members or housemates all know.

To the extent possible choose a workspace that provides sufficient privacy. 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.)

Email

Talk with each survivor about the safety, security, and privacy implications of communicating by email so that they are making an informed decision if they are consenting to email communications.

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 them.

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).

Headphones for phone conversations can enhance privacy for one end of the conversation. If you're using a Bluetooth headset, you may want to keep an extra pair of headphones on hand in case the battery runs out on the headset.

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. Policy should require that staff tell a supervisor immediately if a cellphone (or other electronic device) with PII is lost or stolen. (See OMB Circular M-17-12 for more information on grantee's obligation to have a data breach response policy and to report an actual or imminent privacy breach within 24 hours.)

Always be mindful of where your phone is and who can see the screen when a call comes in. 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, and whether you can control the information displayed. For example, if a survivor's name and/or phone number appear on the home screen it may be best to disable this function. It may also be possible to allow calls to ring through only during the days and hours you establish (e.g., from 8 am to 5 pm, Monday through Friday).

Conversely, be mindful of what information will appear on the recipient's phone if you place a call from your home or work or personal cell phone. Caller ID works automatically with almost every phone service provider. Sometimes you can control this function by 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 are relatively inexpensive ($10 or less) and 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 be saved automatically in your personal cell phone log even if the calls were made or received through an App. If a non-staff member has access to your phone and you cannot disable this function, best practice is to delete the history at least daily for any calls made to or received from a survivor. (Survivors' telephone numbers are almost certain to be PII.) Remember to check the voicemail log on a personal cell phone as a survivor's personal information may appear 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. You may need to tape a piece of paper over the phone screen when the phone is plugged in, to cover any caller's name or number if the phone is located where others can see it.
2. 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!)
3. A long data cord can allow you to plug the phone into a data port but use the physical phone / conduct your conversations in a more private setting.

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.

Similarly, 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 (not every provider offers this option).

Note: 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 include a companion statement or cover letter affirming that the calls were made to and/or received from survivors on the dates indicated.

Remember, too, that 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 signed, written, and informed consent.

<u>Texting</u>

There are many different platforms and apps for texting with survivors or others seeking services. Some helpful issues to consider when deciding what platform(s) to use include:

- Does the survivor have a platform they are familiar with and want to use to communicate;

- Your ability to educate the survivor about the privacy risks associated with the platform options;
- Does the platform offer end-to-end encryption (and is the company considered one of the "ends" or are they limited to you and the survivor); and
- Whether anyone else has access to the survivor's phone and is likely to see (or hack into) the survivor's messages.

At the heart of any form of communication with a survivor is ensuring they can make an informed decision about the risks and benefits.

Videoconference

Videoconferencing presents significant opportunities and privacy risks. It may be the preferred mode of communication for some survivors, but others may prefer phone, email, or texting.

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.

VRLC is not recommending a specific videoconference platform. Each survivor is in a unique circumstance regarding their privacy needs and concerns, the options for where they will appear on video, accessibility requirements, and more. For more information about different platforms and the corresponding security, ease of use, whether they automatically record calls or keep a record, etc., see the NNEDV resource at:
https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5e7e62a25ed80a4219adad77/1585341091261/NNEDV_Communication+Tools_Handout.pdf
and the Oregon State Bar's resource:
https://www.osbplf.org/assets/blog/avideo%20conferencing%20chart1.pdf

Ask the survivor if there is a platform or program they prefer to use. Offer the survivor several options and help them make an informed decision about which program best meets their needs.

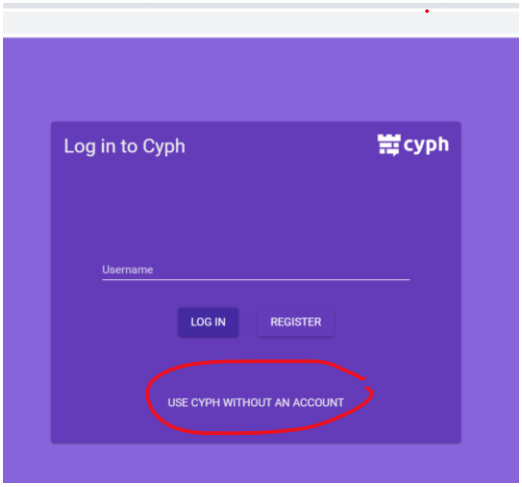
Regardless of what platform you and the survivor select:

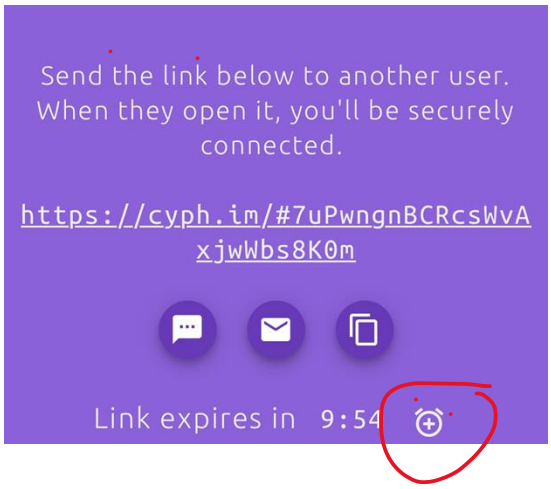
- Before you begin a videoconference with a survivor, make sure they are in a safe and confidential setting, and that it's still a good time for the two of you to meet "in person."
- If the survivor is video calling you from a location where someone might interrupt, discuss in advance what the "cover story" is for the video call.
- Remember that video conferences have audio too! Use headphones if others share your space to minimize 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.
- If the survivor is videoconferencing with you and others, too, remind them to assess what will be visible. (Survivors appearing remotely in court may want to take special care regarding what photos, documents, items, and identifying information in their home will appearing on video.)
- Protect your own privacy too. Be mindful that the person(s) you're videoconferencing with are looking into your home. Take care that you're not inadvertently sharing information you intend to keep private.
- Many videoconference platforms allow the user to insert a virtual background; it can be one included with the program or a photo the user downloads and selects. You may wish to do this to enhance your and your clients' privacy. To guide a survivor through the process of launching a virtual background, it may be helpful to use the "share my screen" function if you are meeting by videoconference.
- Remember that VAWA (and VOCA) are more privacy-protective than HIPAA, so a HIPAA-compliant program does not necessarily meet the VAWA and VOCA privacy requirements.

Do not record a videoconference without a survivor's consent. Similarly, do not save a recording to the Cloud unless both you and the survivor know who will have access to the recording and agree to the storage plan.

For survivors concerned they may be stalked, 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 the resource links above). The platforms referenced here are cited just as examples and are not 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" (see circled area in the photo on the left below). You then send the other user the link to access the service; when the recipient clicks on the link you sent the process to connect the two of you is launched. The default is that the link will expire in ten minutes but you can click on the clock symbol with the + in the center (see red circled area in the photo on the right below) to increase the time in one minute increments. (If you have trouble with the process you can always request another link and start again.)





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.

- **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 third parties, know what is allowed and have a plan for how you will communicate privately.

Practice how to navigate the required software. Discuss how to use the "mute" function or go off-screen while remaining on the call (if permissible).

Scanning

For security reasons, we recommend you only scan documents that contain PII to computers owned by your program, and survivor-related documents are never saved to a personal or shared 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 storing the documents in a locked drawer, closet, file cabinet, or other secure container, or transporting them back to your office (in a safe and secure manner, as discussed above) when they can be disposed of securely. Depending on where you live, weather, and health and safety conditions, burning the torn-up documents may also be an option.

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.

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.

Securing releases of information (ROIs)

Whether you are working from home, your office, or another location, you are still required to meet your VAWA and other confidentiality obligations. Under VAWA, victim service providers may only reveal personally identifying information about someone who sought, received, or was denied services pursuant to: (a) a signed, written, specific and narrowly crafted, release of information (ROI) valid for a reasonable length of time and executed with informed consent; (b) a statutory mandate; or (c) a court mandate.

For a release to be "informed," the victim service provider and the survivor must discuss why the survivor might want specific personally identifying information released and to whom, 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 at a time like this, when many states and tribes have issued "shelter in place" orders that limit in-person meetings, and when so many providers are working remotely. You may need to be creative in how you arrange to have the ROI signed. Some possibilities include:

- Mail or email the survivor a blank ROI for their signature, and after confirming it's safe to do so. Then schedule a time discuss what to fill in. The survivor can sign the completed release and send it back to you. You could include a self-addressed stamped envelope for returning the signed release.
- 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 ROI (or any other documents with personally identifying information) in the mail, it's best to put a blank piece of paper around the documents to enhance privacy in case the envelope is torn in transit. (For more information about mailing documents safely and other data privacy considerations, you may want to review OMB Circular M-17-12 which can be accessed online at: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf.)
- Ask a survivor to print and take a photo of a completed and 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.

- Discuss the ROI by videoconference and ask the survivor to complete and sign the document during your video meeting. They can then return the signed ROI to you by mail, email, etc.
- Mail the ROI to a survivor's trusted friend or family member. Make sure there is no PII anywhere on or in the correspondence unless you already have an ROI to release this information to the friend or family member. Or, you can mail the ROI to the survivor at the nearest post office that will hold mail sent "General Delivery." Be sure to write "hold for pick-up" on the front of the envelope and to include a return address in case the correspondence is not collected.

Remember that the ROI does not have to follow any specific format. It can even be a survivor's signed, handwritten note on a piece of paper. It does, however, need to include all the components of a VAWA-compliant ROI including a reasonably time-limited expiration date.

Electronic signatures: The term "electronic signature" is often used to describe two types of signatures: (1) where the computer inserts a name into a document in a chosen font and (2) a digitized version of the signer's actual signature.[3] The digitized version is preferable because it can be verified more easily, but either is preferable to no signed release at all. A number of different software programs, such as Adobe Acrobat, Eversign, and DocuSign, can be used to securely sign a document electronically. The user will need a touchscreen or stylus to use on their smartphone, tablet, or computer if they plan to physically sign the document electronically. Some programs allow the user to sign a document in any format (e.g., Word, PDF) while others may require the signer to convert the file to a PDF.

While the VAWA (and VOCA)) confidentiality laws have not changed during this pandemic, these are extraordinary times and there may be occasions where it is impossible to get any type of written and signed ROI in a timely manner. For example, a survivor may not have safe access to a printer, smart phone, computer, or other electronic device they can use, the survivor has an urgent need and cannot access services in person to execute the release, etc.

If you can't get a signed ROI, try to get written permission by email or text message to release the PII. The text or email should include the information in a standard written ROI (what information may be released, to whom, for what purpose, and when the release expires).

[3] Although "digital signature" and "electronic signature" are often used interchangeably they are in fact two different formats. While both can be used to sign electronic documents, digital signatures have heightened security because the signature is encrypted.

Sometimes, verbal releases – which are not VAWA- (or VOCA- or FVPSA-) compliant - may be all that you can secure. If you are going to rely on a verbal release, you need to document the basis for the exception and the process you engaged in to ensure the survivor gave informed consent. For example, document in the client file:

- Why the matter is time sensitive and it is not possible to get a timely release;
- That you and the survivor discussed what information is to be released, to whom, and for what purpose;
- When the verbal release expires;
- How you know that the person authorizing you to disclose their PII or release their records is the person they say they are (*e.g.*, you know the survivor's voice; they are able to reference prior conversations between the two of you; they sent a copy of a photo ID);
- If you brought a colleague into the conversation (e.g., a paralegal or legal assistant) to witness the verbal release. (If you do this, take care that your co-worker is not someone whose presence or participation will trigger a mandatory reporting obligation);
- That you informed the client how they can revoke the release at any time; and
- That you asked the survivor to send you written confirmation of the terms and scope of the release at the earliest time it is safe and possible for them to do so.

If you have to rely on a verbal release, arrange for the survivor to reaffirm it in writing as soon as possible.

A verbal release should never be the default option. It should be used only in exceptional circumstances in specific, urgent, case-by-case situations where it is not possible to get a timely written ROI.

Other/Miscellanea

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. Let us know how we can help!

 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.