

Considerations for Remote Consent for the Informed Use of Technology based Communications (Phone, Texts, Individual and Group Video Chats, Email, Electronic Signatures)

Remote informed consent might be needed for survivors who live far away from the program, those who are at work during the program's office hours, and those who may not be able to easily meet in-person for any number of reasons including cases of emergency.

Alternative options, like using phone, text, email and video chat/meetings have issues related that include preventing impersonation, privacy, and safety concerns.

You have the right to private and confidential communications with HCDVCC and the right to accept or refuse sharing your personally identifying information (PII) as follows:

- It's up to you to determine the best way to meet your current need by having HCDVCC disclose personally identifying information (PII) OR NOT, including by technology based communications;
- You are aware of the pros & cons of sharing information (listed below) and communicating via technology based communications, as well as alternative ways to meet the need without providers having to disclose PII;
- These technology based communications (What's app, Go To Meeting, Zoom, Teams, other virtual communication platforms, text, cell phone, email, etc.) will only be used if in person meetings cannot be had, there isn't an ability or enough time to complete a traditional written, and/or signed consent either in person or via mail is obtained;
- HCDVCC can confirm we are actually communicating with the survivor whose PII will be disclosed – see below;
- HCDVCC has clear written instructions on the release form about what information should be disclosed, to whom the survivor wants it disclosed, the method by which it will be disclosed, and the time limit for making the disclosure;
- You were able to review a written version of those instructions on the form before signing it.

Preventing impersonation:

Can we establish a code to be texted or spoken to ensure it's you when using text or phone calls to communicate?

Privacy and safety:

Email is not a secure way to communicate. Abusive partner may have your email password, can you create a new email for our communications? If not, can you erase the emails from my agency from the inbox and deleted box? **Please limit the personally identifying information you send in emails to only what is necessary.** Most email providers (even many of those marketed as encrypted) have access to the content of the emails sent and received by account holders. If they can access the content, then the communication may not be regarded as truly confidential.

Can you let me know when the safe times for communication for phone, text, or video chats are by sending me a text with the code we agree on?

Can you erase all your texting with me right after if you feel the abusive partner will see your phone or is capable of commandeering your phone and looking without your permission?

Abusive partner may have GPS activated on your phone to know your whereabouts – please de-activate.

Abusive partner may have loaded spyware on your cell phone or can trace electronic signature documentation. Please check all apps and security settings.

Technology based communications may be HIPAA compliant but still not completely safe to use. Those cloud based/internet based platforms may have administrators and employees that have access to the communications/use/information shared, so not just HCDVCC staff has access to the information. In addition, their policies may say the company will respond to court orders accordingly which may adversely affect any court proceedings you have or will have with your abusive partner.

I understand all the above technology communications and information/data sharing risks. I understand the below are **not** completely confidential but agree to communicate with my HCDVCC advocate with the platform(s) I choose as follows. I can also choose in person

What's App
 Teams
 Go To Meeting

Zoom Meeting
 Microsoft Teams

email
 cell
 text

Phone 1: _____ Safe to call? No Yes Safe to text/leave message? No Yes

The safe times to contact me are: _____.

Is it safe to e-mail you? No Yes

NNEDV Email best practices:

When Emailing with Survivors

- Let the survivor determine the means of communication that can best accommodate their ability, access, needs, and preferences.
- If a survivor contacts you through email, HCDVCC response should:
 1. Delete their initial email and/or any previous thread. This way, if the email gets intercepted or accessed by the abuser, the request for assistance or the entire history of the conversation isn't revealed.
 2. Include information about the risks related to email communication (example below) and discuss email safety and privacy with survivors, encouraging them to delete the messages they have sent and received, and to clear out their deleted folder.
 3. Ask if there are safer ways that you can communicate.
 4. If communication continues, check in periodically to see if email is still a safe and preferred method of communicating.
- Do not store victims' names and email addresses in address books.
- If you must print out an email exchange, shred the email conversation as soon as you no longer need it.
- Most email programs will autofill the rest of the address for you after you type the first few letters of the name. To prevent sending emails to the wrong person, make sure to double check the address before hitting send.
- Staff should regularly delete emails from survivors so as to not keep identifying, confidential information for longer than needed. This includes purging the "sent" and "deleted" folders as well.

When Emailing Coworkers About Survivors

- Internal communication about survivors should be restricted. Before emailing a coworker about a survivor, consider more privacy focused options, like telling the colleague in person or over the phone.
- Do not include a survivor's name or other identifying information in emails, including initials.

When Emailing Outside Parties About Survivors

Before using email to communicate with outside parties (including using encrypted email), you should first determine if there are other options that are more survivor-centered, and that don't create a digital trail. Opening the door to communicating confidential information over email is very risky. Before doing so, you'll need to make sure that every staff person in your agency who will be using email to communicate confidential client information is fully trained on the VAWA, FVPSA, and VOCA confidentiality obligations, and that they understand the risks and nuances related to email communication. It can be very easy when caught up in the back and forth of an email conversation to forget or accidentally overlook the specific limitations a survivor has set regarding their permission for you to release their information. Advocates can easily share more than they've been permitted to by answering follow-up questions.

If you decide to move forward with using email, be sure to follow the best practices outlined below:

- You can only communicate about a survivor with another agency over email when the survivor wants you to do so, and you can only communicate the specific information they have given you permission to share. When doing this, you must have a written, informed, and time-limited release from the survivor before sharing any information. Refer to the NNEDV Confidentiality Toolkit for more information about releases and confidentiality obligations.
- Make sure that every survivor is fully informed about what sharing their information over email will look like and the related risks of doing so, so that they can make an informed decision about if they want their information shared that way or not. Advocates will need to be prepared to talk about how your agency is working to ensure that the emails are secure, and any potential risks (for example - that you can't control what the other person does with the email once they have it; that they may send a reply to you in an unencrypted format; etc.).

Secure Email

[There are many products on the market that claim to offer secure, encrypted email. Most email providers \(even many of those marketed as encrypted\) have access to the content of the emails sent and received by account holders. If they can access the content, then the communication may not be regarded as truly confidential. For more information about confidentiality requirements for victim services providers under federal law, please see our Confidentiality Toolkit.](#)

A stronger protection is known as "zero knowledge encryption," which makes the data being sent back and forth unreadable to the software company that hosts the email. It is important to know that while this kind of security adequately protects victim data (as long as spyware is not on the device), it also complicates the process of sending and receiving email, so staff and any outside parties will need to be trained on how to use such software.

Agency Best Practices & Policies

Agencies should have a data retention policy ensuring that information that isn't needed is regularly deleted. (Visit NNEDV's Technology & Confidentiality Resources Toolkit for best practices on record retention and deletion.) This policy should include emails received from and sent to survivors, and emails containing information about survivors. Don't forget that emails are often backed up or archived, and email conversations between you and survivors will be saved, so backups and archives containing survivor information will also need to be deleted.

When communicating with others about survivors, make sure you are following your organization's confidentiality obligations and requirements for privilege (if your state has advocate-client privilege). Email is a form of written record; guard it responsibly.

Sample Email Disclaimer Language

Since few people actually read the information in signature lines, being creative in your use of a disclaimer may help get the message across more effectively. The language below can be included at the beginning of every email with a survivor.

Communications between *HCDVCC* and clients are protected by Texas privilege and/or federal confidentiality law. *HCDVCC* does not reveal or share client communications without a client's written permission except where required to do so by mandated reporting.

However, we want to make sure you are aware of the privacy risks related to email communication:

- Email is not a secure way to communicate.
- Emails can be easily seen by other people without your knowledge or consent. Because of that, please limit the personally identifying information you send in emails to only what is necessary.
- *HCDVCC* staff can talk to you more about ways to increase your privacy and safety online.

©2018 National Network to End Domestic Violence, Safety Net Project.

For more detailed safety using technology information, please go to the website below

<https://www.techsafety.org/resources-survivors>

RELEASE OF LIABILITY

I, _____ (client's name), have requested non-shelter domestic violence intervention services for myself and my child/ren (if applicable).

For and in consideration of intervention services provided by HCDVCC, I hereby release and discharge HCDVCC, a non-profit organization, its directors, officers, agents, and volunteers of and from any and all manner of claims, cause of action, debts, or demands, which I, my heirs, successors, or assigns, may have hereafter for claims in connection with personal injury, property damage, theft, any and all claims of any sort whatsoever arising in connection with my services provided by HCDVCC.