NNEDV

Best Practices When Using Email

Many victim service programs use email daily in their work, either communicating with survivors directly or coordinating services with other community programs. By its very nature, however, email is a risky way to communicate. Email can be forwarded accidentally or read by someone it wasn't intended for. The following are best practices for victim service agencies to ensure that their email communication is kept as private and secure as possible.

When Emailing with Survivors

- Don't ban emailing with survivors as a general practice. Although email has risks, refusing to email with survivors isn't the solution. 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, your response should:
    - 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.
    - 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.
    - Ask if there are safer ways that you can communicate. (For some survivors, it may be the only method available to get help, but for others a phone call or in person visit might be safer.)
    - 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 at 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 [agency name] and clients are protected by [state, if applicable] privilege and federal confidentiality law. [Agency name] 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.
> - [Agency name] staff can talk to you more about ways to increase your privacy and safety online.

Supported by US DOJ-OVC Grant # 2016-TA-AX-K064. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.