

NNEDV

Using Zoom: Safety, Privacy, and Confidentiality Considerations

Note: This information can quickly change as Zoom makes changes to their default settings and design. We will update information, as it is available. As a reminder, NNEDV does not endorse any platforms or programs.

With physical distancing measures in place, many organizations and individuals have turned to video conferencing as a way to connect. Zoom has been one of the most asked-about tools. As is the case with any tool, there are going to be benefits and risks for survivor safety and privacy, accessibility, and organizations' confidentiality obligations (how survivors' information is collected, stored, and protected).

As your program chooses tools to use during this time, bear in mind that a tool that works for internal meetings or communicating with community partners may not be a tool that is private or safe for communicating with survivors.

Here are some quick summary points about Zoom:

- Offers video chat for one-to-one or groups. Free and paid plans.
- Access:
 - Strong on accessibility for Deaf users; allows for closed captioning and ASL interpretation.
 - As with any video, internet access and bandwidth may be a barrier.
 - New users are asked to download an app and there may be safety or accessibility barriers. New downloads may be seen by the abusive person.

- Privacy:
 - End-to-end encryption is not currently offered. This means that the content of chat or a recorded video, for example, is not encrypted on Zoom’s servers.
 - Not the most private/data secure by default; for added privacy an additional agreement (BAA) between agency and Zoom is required and may require an additional fee.

Audience	Zoom – standard	Zoom – with BAA	Use security options
Survivors	NO	OK Assess for accessibility; Informed consent required	YES Don’t require “authenticated” user or identifying info; Meeting title shouldn’t include advocate’s name or mention services
Staff, volunteers or community partners	OK Don’t share survivor PII	YES Don’t record if sharing survivor PII	YES Password required
General public	YES	YES	YES Password required, participants are muted by default and can’t share files or screens

Using Zoom to Communicate with Survivors

By design, Zoom functions best by having each user download an app and create an account using an email address. For survivors, this can pose a safety or privacy risk if the abusive person is monitoring the survivor's devices or accounts. Since Zoom is a popular app right now, this may not necessarily pose a risk, but it is important to help survivors assess their risks and plan for safe use of this or any other app. You'll also want to discuss any potential barriers due to internet bandwidth or other tech issues.

Joining a Zoom meeting from a web browser, without downloading the app, is possible, but the host must select a "Join from your browser" option in the Zoom web portal [*found under Settings → In Meeting (Advanced)*] when setting it up. If this isn't done, the person will not be allowed to join without downloading.

Zoom has good options and functionality for accessibility, specifically for people in the Deaf community or who are hard-of-hearing. Many video windows can be displayed during a meeting or chat, providing the ability to have multiple interpreters. Zoom also offers a built-in closed caption option at the bottom of the screen. The host is able to assign a trusted attendee to type the captions, which can be a hired captioner, or someone else in the meeting. After completing the meeting or webinar, a file with the captions can be downloaded to the computer of the meeting host. Captions are not saved to the Zoom cloud. All attendees will be able to save the captions, if enabled by host [*in Zoom web portal, found under Settings → In Meeting (Basic)*].

Just as it is with in-person advocacy, it's important to be survivor-centered when communicating remotely. The best tool to use is the one that works best for the survivor you are working with. One survivor may prefer to talk on the telephone while they are taking a walk outside. Another may prefer text or chat because it is

a quiet way to communicate if the abuser is nearby. Someone else may prefer video because they like the sense of personal connection.

To help a survivor decide what tool is best for them, discuss the safety of their devices and surroundings. Offer a number of ways to communicate, including a phone call, the audio-only option in the web conferencing service, online chat, or text messaging. Once you've helped with the privacy and safety planning process and provided options for communication, respect their choice about which tool best meets their needs. Prepare tips and information to share with survivors about how to use the various tools you have available. And be sure to test the technology to make sure it works properly before meeting with survivors. Read more about [Best Practices for Digital Services](#).

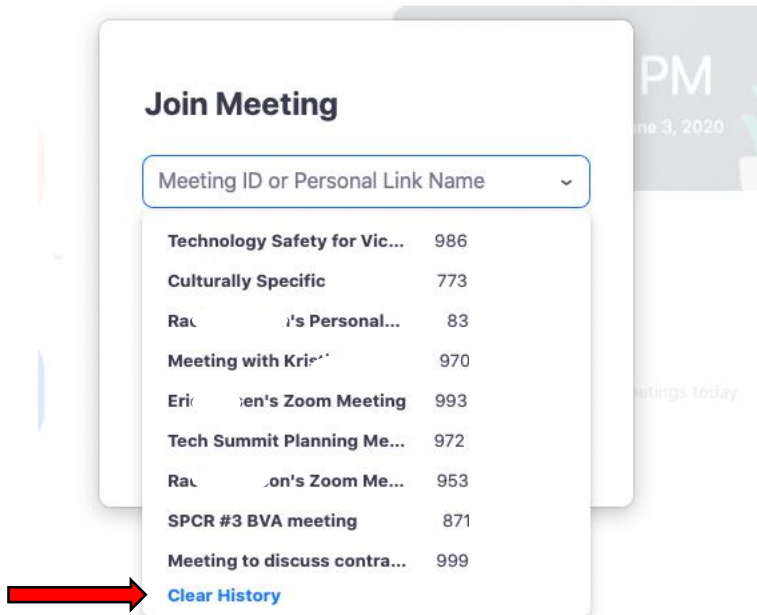
Zoom Privacy & Data Collection

By default, Zoom collects personally identifying information (PII) of users, including the internet (IP) address of each user and their email address if they supply that to Zoom. Zoom's HIPAA Business Association Agreement (BAA) option stops Zoom from collecting PII. However, this option may be costly, and therefore financially inaccessible for some programs. For more information, please see the BAA Zoom Option section below.

Chat in Zoom is not end-to-end encrypted by default. Without that, the content of chats may be visible to Hosts under Chat History, posing a significant privacy and confidentiality risk. To make sure end-to-end encryption is turned on for chat, follow [these steps provided by Zoom](#). Video is not end-to-end encrypted and the option does exist for Zoom employees to intercept and join calls (they will be visible in the participant list).

Programs should be mindful about how they label meetings or advocacy sessions with survivors. The name of the session can show up in recent meetings and if

survivors are being monitored can identify to abusers that the survivor is seeking help, or disclose the name of the advocate or program.



To learn more about Zoom’s policies, check out their [Privacy Policy](#) .

Federal Confidentiality Obligations

VAWA (Violence Against Women Act), VOCA (Victims of Crime Act), and FVPSA (Family Violence Prevention and Services Act), prohibit sharing any survivor PII unless the survivor explicitly asks the program to do so through an informed, written, time-limited release of information.

The Health Insurance Portability and Accountability Act (HIPAA) addresses the sharing of patient health information, specifically as it relates to payment for services. HIPAA is designed to share information between health care providers and insurers. **If your program receives VAWA, FVPSA, or VOCA funds, “HIPAA compliant” is not sufficient.**

For more information on the differences between HIPAA and VAWA, VOCA, FVPSA, read our [Frequently Asked Questions About U.S. Federal Laws & Confidentiality for Survivors](#) and [FAQs for Victim Service Programs About HIPAA Privacy, HIPAA Security, and Technology](#).

Please note: Safety Net cannot endorse products or certify products as “VAWA compliant.” Assessments of products or platforms should focus on whether the product or platform allows you to ensure the level of confidentiality you need to work with survivors.

Your program’s confidentiality obligations pertain to information that survivors entrust with you. It’s important to double-check that survivor information you hold is not being shared with the technology provider. With any communication tool, survivors can make their own choices about what information they share with the company providing the service, as long as they have the information to do so. If a company is collecting PII directly from survivors, it’s important that you inform survivors prior to use to ensure that they can make an informed choice about their own privacy.

Zoom BAA Option

Zoom’s HIPAA Business Association Agreement (BAA) option does offer additional privacy protections for users. With the BAA option, which starts at about \$200/month, encryption is enabled for all members of the account, video and chats are end-to-end encrypted, cloud recording is disabled, and device and user information logging and reporting is removed. Additional information on the Zoom BAA Option can be found [here](#).

Note that all users are urged by Zoom interface to download the app, and to create an account. If a survivor does either or both of those things, they are

sharing personal information with Zoom, though not necessarily in relationship to receiving services from your program.

Zoom is not certified, meaning no one is policing these features and they could be subject to change. [Learn more about Zoom and HIPAA.](#)

Preventing “Zoombombing” or Meeting Hijacking

Zoombombing is when malicious actors join and hijack a meeting by posting explicit content or trolling the meeting. Zoom-bombings can be traumatizing for survivors and others as many instances of this have included taking over the screen to display hateful, violent, and racist content.

Zoombombing is only an issue when a link for a meeting is shared publicly and there are settings to prevent it from happening. **It’s important to note that we should NOT be using public links to provide services to survivors.** Even with these settings in place, the public option functionality is not one that is meant for such sensitive, private information and disclosures.

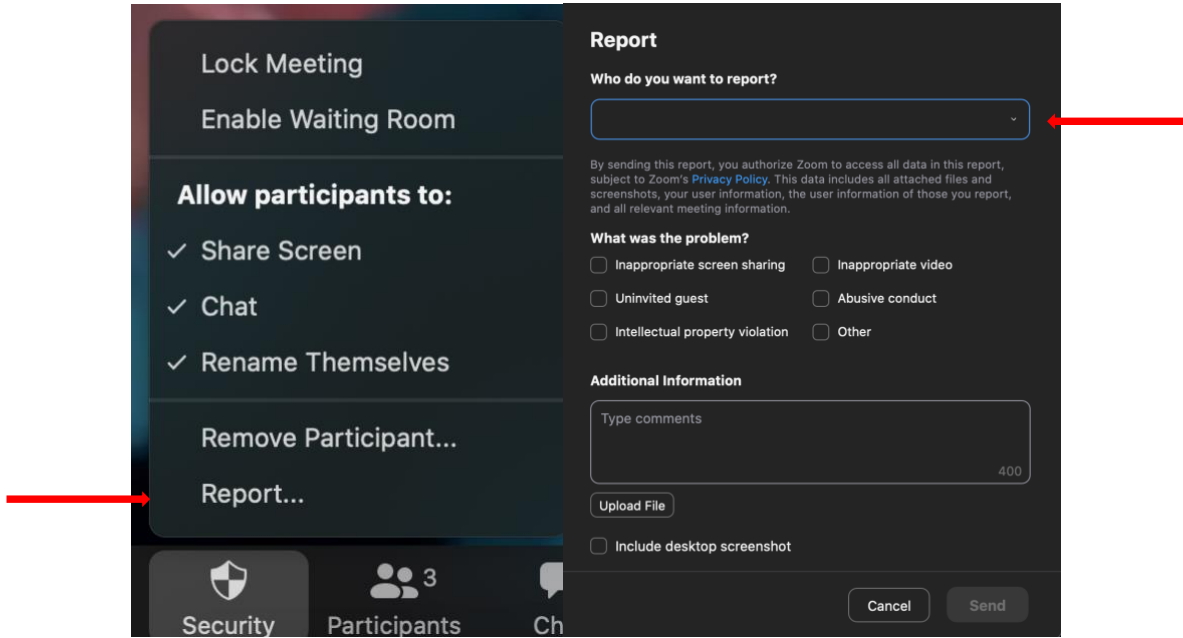
The only scenario where Zoom could be used in this way (publicly where you have to consider Zoombombing prevention) is for online support groups that are open to the public. There are many concerns about hosting support groups in this way, please see our handout on [Online Support Groups](#) for more information.

Individual calls with survivors should never be shared publicly. Sharing links publicly offers hijackers/trolls the quickest way to access these meetings. If possible, only share the link to a meeting with known participants and do not make it public. Participants should be advised not to share links without approval to minimize the risk of hijackers accessing meetings.

If you are using Zoom and sending links publicly, follow the below settings to prevent Zoombombing:

- Require a password when scheduling new meetings [*found under Settings → Schedule Meeting*]
- Mute participants upon entry [*found under Settings → Schedule Meeting*]
 - Host can control whether participants can unmute themselves.
 - Host has ability to individually unmute participants in the meeting.
- Disable File transfer [*found under Settings → In Meeting (Basic)*]
 - This prevents the host and participants from sending files through the in-meeting chat.
- Control Screen Sharing [*found under Settings → In Meeting (Basic)*]
 - Change from All Participants to Host Only. This prevents someone from taking over the screen and displaying their content.
- Control Chat [*found under Settings → In Meeting (basics)*]
 - Turns off ability for meeting participants to send a message visible to all participants.
- Prevent removed participants to rejoin [*found under Settings → In Meeting (Basic)*]
 - Make sure this is not enabled. If the host has to remove someone during the meeting, this prevents them from rejoining.
- Establish a Waiting Room [*found under Settings → In Meeting (Advanced)*]
 - This allows the host and co-host to monitor and control who is joining the meeting.
- Create a unique meeting ID [*select “Generate Automatically” under Meeting ID when scheduling a meeting*]
- Report a user as a host [*select “Security” at the bottom of the screen then select “Report”*]

- Then select the user and fill out the appropriate information detailing why the person is being reported.



All of these options can be found in the Zoom web portal under Settings.

Registration

Requiring people to register ahead of time will provide you with a list of people to review prior to the meeting. Each registrant will receive an individual link to join the meeting and after the meeting, you can receive a list to see who joined. This is an option for meetings and not for services with survivors. The individual link received after registration is only for the person that registered. It cannot be used for multiple people to access the meeting. If you are concerned with who may be registering, you can also change the registration to require manual approval. This means that as the meeting host, you will need to approve or reject a registrant before they receive information on joining the meeting.

Manage Attendees	Registrants: 0	View
Registration Options	Automatically Approved	CLICK! Edit
	<input type="checkbox"/> Send an email to host	
	<input type="checkbox"/> Close registration after meeting date	
	<input checked="" type="checkbox"/> Show social share buttons on registration page	

Registration ✕

Registration

Required

Approval

Automatically Approve

Registrants will automatically receive information on how to join the webinar.

Manually Approve

The organizer must approve registrants before they receive information on how to join the webinar.

Any link to join a meeting or group with survivors should never be posted publicly. These meetings should be sent directly to the survivors joining or require them to register to receive a link to join, keeping in mind that registering does require survivors to provide PII to Zoom. Manually approving attendees for these meetings may be important to ensure only survivors are joining and that the registration didn't go to a wider audience. If you are holding weekly groups with survivors in Zoom, there is an option to make the meeting recur daily, weekly, or monthly, so survivors don't have to re-register each time.

Controlling Attendance During the Meeting

Even if you've updated your settings and have been cautious with sharing your meeting information, it's possible that a bad actor gets into your meeting. This is where turning off the screen share function for everyone but the host, disabling file sharing, and even disabling the public chat is critically important. But there are a couple additional things you can do to prevent unexpected trolls from taking over. Once a meeting or chat begins, you have the ability to lock the room and prevent anyone else from joining. Under "manage participants," at the bottom of the screen, choose "more" then "lock room." This may be challenging if you have people that have to drop off the meeting for a period of time and want to come back. This could also be problematic if a survivor is locked out of the support group they were planning to attend. If you don't want to lock the meeting room, you have the ability to remove someone from the meeting. Under "manage participants," hover over the name of the person you want to remove. When options appear, select "remove." As long as the "*Allow removed participants to rejoin*" option is disabled, the person removed will not be allowed back into the meeting.

Recently, Zoom has added a couple new security features. They have enabled passwords and virtual waiting rooms as the default for the Free Basic and Single Pro License Zoom users. As service providers, it is our responsibility to make sure any program or platform we are using is allowing for a safe space. We can also help survivors understand Zoom settings when they are using the platform to connect with friends, family, and co-workers.

Recording Settings

NOTE: Conversations with or about survivors should NOT be recorded. If you will be recording any meetings, chats, or webinars, there are a few recording features to be aware of regarding privacy and data collection: cloud vs. local recordings,

chat function, [closed captioning](#), and [automatic transcription](#). It's important to note that prior to beginning any recording, participants should be notified by the host that the session will be recorded and it's possible their information could be included in that recording, including their name.

When it comes to recording, there are two options: cloud and local. Cloud means Zoom will record to their cloud service and participants can download the recording after. Local means the recording will be saved directly to your computer. Any recording saved to the cloud via Zoom can be accessed by Zoom. Any recording saved locally or to your computer can only be accessed by you.

While the chat function can be end-to-end encrypted (if enabled – click [here](#) for steps to enable), there is still the ability for other attendees to save the chat. By default, the chat is automatically saved to the meeting host's computer [this can be turned off in the web portal under Settings → In Meeting (basic)]. However, unless disabled, other attendees of the meeting or webinar are able to download the public chat (messages sent to the entire group). While the information in the chat on the Zoom platform is encrypted, the information is no longer protected if someone downloads the chat and is able to share it. For meetings and webinars that are recorded to the cloud, the chat will be saved to the cloud unless turned off in the Zoom web portal under Settings → Recording.

NOTE: If you are communicating with a survivor and the chat transcript is saved to your work device, be sure to delete the transcript. This should be treated as any other communication with survivors and not be saved.

Profile

Meetings

Webinars

Recordings

Settings

Account Profile

Reports

Attend Live Training

Video Tutorials

Knowledge Base

Meeting

Recording

Telephone

Recording

Local recording

Allow hosts and participants to record the meeting to a local file

- Hosts can give participants the permission to record locally

Cloud recording

Allow hosts to record and save the meeting / webinar in the cloud

- Record active speaker with shared screen
- Record gallery view with shared screen ⓘ
- Record active speaker, gallery view and shared screen separately
- Record an audio only file
- Save chat messages from the meeting / webinar

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other

In Meeting (Advanced)

Breakout room

Allow host to split meeting participants into separate, smaller rooms



- Allow host to assign participants to breakout rooms when scheduling ⓘ

Remote support

Allow meeting host to provide 1:1 remote support to another participant



Closed captioning

Allow host to type closed captions or assign a participant/third party device to add closed captions



Save Captions

Allow participants to save fully closed captions or transcripts



For business, education, and enterprise Zoom accounts, by default, transcripts are prepared for meetings and webinars are recorded to the cloud. Depending on the content of the meeting, this could be recording PII and other personal information of survivors. For example, if your organization decided to hold an internal meeting and recorded it for staff that were not present, content discussed is transcribed. However, there is a way to turn off the automatic transcription in the Zoom web portal under Settings → Recording.

The screenshot shows the Zoom web portal's Settings page. On the left is a navigation sidebar with options: Profile, Meetings, Webinars, Recordings, Settings (highlighted in blue), Account Profile, and Reports. Below this are links for Attend Live Training, Video Tutorials, and Knowledge Base. The main content area has three tabs: Meeting, Recording (selected), and Telephone. Under the Recording tab, there is a 'Recording' section. It includes 'Local recording' (allowing recording to a local file) with a checked option for 'Hosts can give participants the permission to record locally'. 'Cloud recording' (allowing recording to the cloud) has several checked options: 'Record active speaker with shared screen', 'Record an audio only file', and 'Save chat messages from the meeting / webinar'. 'Advanced cloud recording settings' includes checked options for 'Display participants' names in the recording', 'Record thumbnails when sharing', 'Audio transcript', and 'Save panelist chat to the recording'. Unchecked options include 'Record gallery view with shared screen', 'Record active speaker, gallery view and shared screen separately', 'Add a timestamp to the recording', and 'Optimize the recording for 3rd party video editor'.

Before deciding on a product or platform, we encourage programs to read [Using Technology to Communicate with Survivors During a Public Health Crisis](#) resources in the [Digital Services Toolkit](#). This will help you determine the types of services

you want to offer to best meet the needs of survivors and the communities you work with. Our [Video Conferencing & Digital Communication Platforms: Comparison Chart](#) is another resource that will help you compare different tools and make an informed decision.

© 2020 National Network to End Domestic Violence, Safety Net Project. This product was supported by cooperative agreement number 2019-V3-GX-K017, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this product are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

We update our materials frequently. Please visit [TechSafety.org](https://www.techsafety.org) for the latest version of this and other materials.