Digital Written Consent to Share Information

This document discusses best practices related to the use of digital tools to obtain written consent to share information. Before reading this document, we strongly encourage you to review how to work with survivors regarding the release of personal information and what the law requires related to survivor privacy and confidentiality.

Why Written Consent is Important

Federal confidentiality guidelines require that when survivors want a victim service program to share information about them with a third party, the program must first obtain informed, time-limited, written consent.

The informed, time-limited, written consent rule is intended to:

1. Highlight for both survivors and providers that the information belongs to the survivor;
2. Record clear instructions for providers so they know exactly how and when the survivor wants their information shared;
3. Protect against impersonation and prevent others from gaining access to survivor information without their consent; and
4. Provide backup documentation that the information was shared at the survivor's request.

Neither the Violence Against Women Act (VAWA), the Family Violence Prevention Services Act (FVPSA), nor the Victims of Crime Act (VOCA) define the term "written," but it is generally understood to mean a document signed by the survivor that outlines their instructions for how, when, and with whom they want their information shared. While the safest and most private option for many survivors may be meeting in-person, developing alternative ways for consent to be obtained remotely is important.

Remote 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. When identifying alternative options, it's important to remain survivor-centered in the process and talk through issues related to preventing impersonation, and how to navigate privacy and safety concerns. There are ways that programs can both provide survivor-centered options that help ensure the survivor's needs are met, while also following best practices related to confidentiality.

Determining if Digital Written Consent is an Option

Below is a helpful checklist to help determine if digital written consent makes sense. Note that all of the items in this list should be in place and be applicable to the situation in order for digital written consent to be an option.

- √ The survivor has determined that the best way to meet their current need is to have the provider disclose personally identifying information (PII);
- √ The survivor is aware of the pros & cons of sharing information, as well as alternative ways to meet the need without providers having to disclose PII;
- √ There isn't an ability or enough time to complete a traditional written, signed consent either in person or via mail;
- √ The provider can confirm they are actually communicating with the survivor whose PII will be disclosed;
- √ The provider has clear written instructions 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;
- √ The survivor either wrote those instructions or reviewed a written version of those instructions; and
- √ The provider has a record that the survivor has approved the instructions.

Basically, providers must:

1. Know WHO they are communicating with;
2. Know WHAT the survivor wants disclosed;
3. Know HOW the survivor wants it disclosed;
4. Know TO WHOM the survivor wants it disclosed;

5. Know HOW LONG the provider has to make the disclosure;
6. Have a WRITTEN set of instructions that can be saved and referred to later; and
7. DOCUMENT that the instructions came from or were approved by the person whose information is being disclosed.

Choosing a Digital Tool

Digital tools like email, text, and chat allow survivors to communicate with providers and send instructions from a distance. Every tool has privacy and safety related risks that advocates should inform survivors about before they use it to send personal information to advocates. Once a survivor understands the risks, they can decide if they feel it's safe enough for them to use, and create a plan for purging the information to decrease the chance that it will be seen by someone else without the survivor's permission.

A tool should never be used if it doesn't feel safe to the survivor; instead, alternative options should be explored. Advocates should also implement best practices related to confidentiality obligations and their agency's use of technology, to ensure that survivor information is properly protected and stored. (For more information on the use of technology to communicate with survivors check out our Digital Services Toolkit, and for more information on confidentiality obligations check out our Confidentiality Toolkit.)

Getting Ready

Any process for obtaining survivor consent to disclose information must meet the following criteria:

- The process should foster survivor choice and true informed consent. Use the Advocate's Instructions document to help guide the conversation and determine if, when, to whom, how, how much, and for how long information will be disclosed by a provider on behalf of a survivor;
- Confirm that the survivor is the person instructing disclosure of information;
- Obtain the survivor's signature (or other form of affirmation that is intended as a signature by the survivor and is recognizable to both the survivor and the provider), which confirms the instructions are correct and approved by the survivor; and

- Preserve the instructions for future review in case of uncertainty or disagreement.

Providers should develop a routine set of questions that mirror their release form. This can be pasted into a chat, text or email and filled in by a survivor when they want the provider to disclose their information. Generally, the digital written consent should be accompanied by a second method of authentication, such as a phone call with the survivor, or the use of a pre-determined code word or phrase, to confirm their wishes.

For more information about confidentiality, check out our Confidentiality Toolkit.

Thank you to our grant partner Alicia Aiken, JD, from the Danu Center's Confidentiality Institute, for her extensive contributions to the creation of this document.

Supported by US DOJ-OVW Grant #2019-TA-AX-K003. 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.