Co-funded by the
Erasmus+ Programme
of the European Union

DISCO
Development of "at a Distance" Counselling Skills for professionals in the field of Counselling Women Victims of Violence or Abuse

Agreement Nu.: 2017-1-EL01-KA202-036170

Some considerations when using online/distant technology for service provision

Compiled

By Dr Maria Pentaraki, QUB

Participating Organisations:

Nexus NI
rape & sexual abuse support

QUEEN'S UNIVERSITY BELFAST

M&M

UNIVERSITY OF TARTU

Tartu Women's Shelter
Violence is not the way out.
There is a way out of violence.

WAVE

UNIVERSITY OF CRETE

Union of Women Members' Associations of Heraklion Prefecture

ΠΑΝΕΠΙΣΤΗΜΙΟ FREDERICK

Some considerations when using online/distant technology for service provision

Is the platform safe?

You need to consider the safety of the platform you are using, as any technology can be hacked. How easy can it be for someone to hack the platform to have access to the conversations taking place?

Are the data accessible by other people outside the agency?

Services provided through a third party, could allow others outside of the agency access to the information shared on or through the service. Agencies need to know how and what their staff has access to. When selecting a service, know exactly what information is collected and for what purpose.

Is there a possibility to keep records based on the technology used?

As records may be released to law enforcement or to an attorney through a court order or subpoena, **it is very important to know** if the service you have selected allows record keeping of any kind. Also, it is important to know if these records once they are deleted by the clients and the agency, permanently disappear or some further action is needed from the service provider. Consider developing a protocol in terms of record keeping, taking into account the legal context of your country as well as protecting the confidentiality of the service users.

If there exists a possibility of a breach of confidentiality, conversations should not be recorded. They should be deleted immediately along with contact information (if the contact is through a hotline). Agencies should not retain the phone numbers or the conversations. Do not store any information.

Any email sent by a survivor should not be kept longer than needed, it should be deleted as soon as possible so as not to keep offering the possibility to a third party to identify confidential information. This should include clearing the “sent” and “deleted” folders too.

Is someone impersonating the survivor?

Online/distant technology allows the danger of impersonation. It might be useful in order to ensure the identity of the other person and avoid impersonation to create a code word or phrase.

Some additional online safety tips for victim service agencies

1. **Add a safety alert header to your website. It can be at** the top of every page on the agency website, because you never know which page a survivor will visit first. Decide what will the safety alert contain: It can be something like the following:

If you are in danger call the police (provide number) or use a safer computer or call your local helpline (provide number).

Include an emergency ESCAPE button that redirects the web browser to a less risky content by linking it to a random website such as weather or news that loads quickly. An Escape button allows a survivor to switch to a random webpage quickly if someone enters the room. However, it does not delete web browsing history.

2. **Remove email addresses from the agency website and use web forms instead.** Web-based contact forms are often safer for survivors to use since the communication happens within the website (instead of through the survivor's email account where the emails might be monitored by the perpetrator). **The form could include questions** about the safety of reaching back out to them. The above are adopted from The Safety Net Project of the National Network to End Domestic Violence. Please visit: https://www.techsafety.org/agency-website-safety-tips for additional tips.

A Things to do list for Agencies (Southworth, et al 2005:11-12):

1. "Revise organizational communication, records, and confidentiality policies to include technology security issues.
2. Update organization website safety information for victims searching for support online. Also, ensure that your website is accessible to all survivors, including individuals with disabilities who use assistive technology such as screen readers.
3. Create organizational policies that address how (or if) to respond to emails from victims. When reviewing policies, consider the possibility that abusers may be

monitoring the victim's email account or computer, so policies should focus on how to increase safety and always provide informed consent.
4. Increase victim safety by securing survivor data. Only store victim information on computers that are not connected to the Internet or networked to the Internet. If using an Internet-based database for victim records, designate a computer to use only for that purpose. To minimize hacking and SpyWare risks, do not store other victim files on that computer or use it for email or Internet browsing.
5. Given that abusers work in every field and some are extremely skilled in using technology, evaluate data collection and sharing policies to keep victim data out of the hands of stalkers, abusers, and members of the public".

Strategies for Advocates (Southworth, et al 2005):

1. "Identify training opportunities on technology investigation, computer forensics, or prosecution, and attend these trainings with law enforcement or prosecutors from your community. Many states have computer crime units or prosecutor associations that may be available to support and train local jurisdictions.
2. Identify the police and prosecutor technology crime specialists. If the community does not have a technology unit, identify officers and prosecutors with technology experience. Discuss how law enforcement process digital evidence and conduct investigations.
3. Work with law enforcement to identify what evidence is needed, so advocates can work with survivors to document the necessary information. Encourage officers and survivors to discuss how the investigation will impact the victim's life. For example, if a victim's computer is seized, it may be possible to duplicate the hard-drive and return it quickly.
4. Work with the legal system to identify the state laws that could apply to emerging technology strategies of stalkers. Some stalking laws only include electronic communication devices, so prosecutors may need to use eavesdropping or other statutes to address some crimes.
5. Ask that prosecutors discuss the potential consequences with a survivor of pursuing a technology related criminal charge compared to a domestic violence or stalking charge, so that she remains informed of how potential media coverage and evidence collection practices might impact her life. For example, … media covered the Michigan SpyWare and the Wisconsin GPS stalking cases.
6. Join community committees discussing Internet publication of court or voter records and advocate for privacy provisions for survivors".

Bibliography –

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, violence, & abuse*, *19*(2), 195-208.

Henry, N., & Powell, A. (2015). Embodied harms: Gender, shame, and technology-facilitated sexual violence. *Violence against women*, *21*(6), 758-779.

Mason, C., & Magnet, S. (2012). Surveillance studies and violence against women. *surveillance & society*, *10*(2), 105.

Southworth, C., Dawson, S., Fraser, C., & Tucker, S. (2005). A high-tech twist on abuse: Technology, intimate partner stalking, and advocacy. *Violence Against Women Online Resources*.

Southworth, C., & Tucker, S. (2006). Technology, stalking and domestic violence victims. *Miss. LJ*, *76*, 667.

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence against women*, *13*(8), 842-856.

Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. Violence against women, 23(5), 584-602.

The Safety Net Project of the National Network to End Domestic Violence (USA), develops resources and information on the use of technology for agencies and survivors of domestic violence, sexual assault, stalking, and trafficking. On their web page they have toolkits that contain a variety of information that can be helpful for victim service agencies as well as survivors. https://www.techsafety.org/resources/ Please, visit these resources in order to be fully informed.
Additional resources can be found at:
https://hackblossom.org/domestic-violence/ This is an excellent comprehensive website which provides technical support to survivors of domestic violence.
https://hackblossom.org/cybersecurity/ They offer an excellent DYI guide on feminist cybersecurity which has concrete advise on how to protect digital spaces.
Accessnow.org They run a helpline on digital security.