Confidentiality in the Time of COVID-19

Rob (Roberta) Valente

Domestic Violence Policy and Advocacy

Goals of this webinar: Delivering services during the COVID-19 pandemic

Goals	At the end of this webinar, victim advocate participants will learn about serving survivors during the pandemic:
Survivor privacy	Have a refreshed understanding of confidentiality and privilege
Use tech safely	Learn about confidentiality protections—or lack of them—when using technology to deliver services
Manage info	Understand the best ways to manage information
Support survivors	Be of support to survivors in other settings

Goals: Why are we here today?

- Helping survivors heal
- Helping survivors find safety
- Helping survivors find stability
- Helping survivors obtain justice
- Being the best advocates we can be

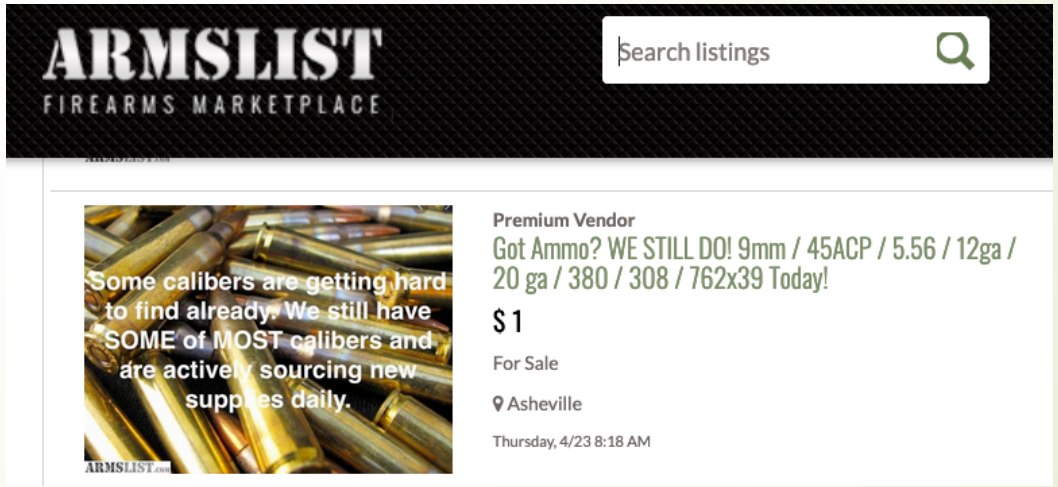
Stay-At-Home policies create enormous danger for many survivors of domestic violence

- Usual "relief valves" are not available
  - Abuser is out of work/telecommutes, home all day
  - Survivor is out of work/telecommutes, new opportunities for abuser to exert control
  - Threats of/accusations about infection
    - Abuser demands survivor not use PPE or sanitizing protocols
    - Abuser accuses survivor of not taking appropriate care to avoid infection
  - Threats about cutting off access to health insurance or medical care (COVID-19 related or separate from)
- Abuser's frustration leads to heightened abuse
- Co-occurring danger to children

COVID-19 has made it far more likely that abusers have access to a firearm in a domestic violence situation

Background checks are up, indicating increased sales by FFLs

- According to the FBI, 3.7 million background checks were done in March 2020-–the most for a a single month since the system began in 1998. ABC News, April 1, 2020
- July 2020 gun sales are the highest on record



Confidentiality is so important to survivors!

- Survivors will not be able to heal and move forward if they cannot first have a "safe" space to explore what has happened and learn about their options
- Survivors cannot engage in counseling and assessing options if they believe their conversations will be overheard or disclosed
- Even during a pandemic, survivors need confidentiality

What do survivors need to be able to talk with us?

What does empathy look like?

- Understanding how survivors feel
- Non-judgmental


RSA
SHORTS

What does trust look like?

- Trust is difficult
  - We often decide whether to trust someone within the first few seconds of meeting them

When they trust us, what do survivors expect from us?

- Assure survivors we have expert knowledge that will help them
- Show survivors we are able to listen carefully
- Let them know that in spite of their past experiences with untrustworthy people, we will strive to maintain their trust
- **Let them know that whatever they say to us will remain *confidential*.**

What is Confidentiality?

- Ethical duty
- Can arise when client divulges information to certain professionals
- Information that is meant to be held in confidence or kept secret
- Statements that are meant only for the ears of the person addressed
- Can only be disclosed with client consent, subpoena or court order

What is Privilege?

- **Privileged communications are protected by law**
- Common examples:
  - Attorney-client privilege
  - Social work-client privilege
- Generally immune from subpoena and court order
  - Can only be released with consent of client
  - Can be used to resist release of information
  - Recognized by law enforcement and courts (also tribal government & agencies)
- Statutory exceptions:
  - Mandatory reporting
  - Threat of imminent harm or danger to self or others

PRIVILEGE PROTECTION MAY BE WAIVED

- Third party in the interview room
- Providing information to third parties not protected by statutory privilege
- Information is available in other public forums

- This is so important during the COVID-19 pandemic!
- When doing remote services, it is so easy to inadvertently waive the survivor's privilege

The Basics of Confidentiality

- Do not share personally identifying information with anyone outside of the victim services program, except:
  - In cases of emergency
  - Unless the program obtains consent from the survivor. The consent must be:
    - Voluntary
    - Informed
    - Time- and activity-limited
    - Signed by the survivor

Who "owns" the information a program has?

- Any information the client shares with your program "belongs" to the client. This includes:
  - Case notes
  - Intake information
  - Forms filled out by the client
  - Conversations
  - Phone calls, texts and emails, including records that they happened

- **Remember**—once confidential information is released to a tribal government agency, that information may become part of the public record and visible to other tribal government personnel—and perhaps even members of the public. It can never be private again.

- *Example: A victim advocate may share information about the survivors' confidential location with a victim assistant. What was confidential for the victim advocate may become part of a law enforcement investigation concerning parental kidnapping once shared with a victim assistant.*

VAWA Confidentiality (34 U.S.C. 12291(b)(2))

"Nondisclosure of confidential or private information"

- Any tribe or tribal organization that receives VAWA funding, whether through CTAS or through discretionary grants, must agree to keep communications with survivors confidential.
- Tribes or tribal organizations receiving VAWA funding can't share survivors' names, addresses, phone numbers, or any other information that might reveal the survivor's identity.
- The program cannot release any information they receive from a client without informed, time-limited, written consent.

Confidentiality & Remote Intake/Services

- **Before taking any information, make sure client knows what your confidentiality policies are:**
  - Usually the client controls the information collected
  - It cannot be shared unless subpoena, court order or informed, written consent of client
  - Your program is committed to using the most private, safest technology for communications

Confidentiality & Intake/Services

- **Make sure the client understands the limits to confidentiality**
  - Mandatory reporting
  - Imminent danger: threat to self or others
  - Court order or subpoena (program will try to limit disclosure)
  - Information saved or exposed by technology
  - Sharing data in the aggregate with funders

Basic rules of using technology for remote services

- There are two sides to every communication
  - You can manage confidentiality on your side of the technology
  - It is much harder to manage confidentiality on the survivor's side
  - Part of safety planning is teaching the survivor to delete records on technology
- Technology can be intercepted if the abuser has access
  - Many forms of technology create records: who was contacted and when, which the abuser can track via phone bills or computer histories, etc.
  - Many forms of technology create records of the content of the communication that stay on equipment the abuser may access
- Survivors and victim advocates should make every effort to delete records of communications, especially where the abuser may have access

The Limits of Technology

- Technology is designed to make a record of communications
- The older the technology, the safer it is:
  - Landline phones
  - Mail
- The newer the technology, the less safer it is:
  - Cell phones
  - Texting
  - Email
  - Videoconferencing
  - Chat

Older technology

- **Landline phones**
  - Keeps record of calls made and times
  - Usually need a subpoena to get this information
  - Preferable for counseling or other communications that are confidential
  - Can be overheard, but once call ends, no trace
- **Regular mail**
  - Only record is postmark on the envelope and date on correspondence
  - Need a subpoena to get this information
  - Preferable for sending sensitive information, like filled out forms
  - Can be intercepted by abuser if not sent to alternate address
  - Is a very slow method of communication

Newer technology: Cell phone calls

- Generally safe to conduct confidential communications on a cell phone call: no record of what was discussed
- Note that number and time called are recorded by phone company and may appear in the phone bill, particularly paper copy in mail
- Caller ID may alert abuser
- When the survivor has to shelter in place with the abuser, communications may be overheard, so important to develop "safe" words
- Another privacy option is for survivor to "lock" phone, unless it is not safe to do so because of abuser control or retaliation
- Tracking and recording devices are possible if abuser has access to phone
- Voice mail is a record that may be intercepted or overheard by abuser
- Technically, if the phone is in survivor's name, what's on the phone is controlled by survivor; if phone is on abuser's plan, abuser will have access to call records

Newer technology: Texts

- Survivors may prefer texting to talking out loud on the phone when sheltering in place with abuser
- Texting is not safe because it leaves records of actual texts and time that texts were sent and delivered
- If using text, use following protocols:
  - Encourage survivor to delete all text message exchanges as soon as communication is finished so not visible on phone (note that phone company may still have records of the texts that can be requested by account owner or obtained by subpoena)
  - Encourage survivor to have own phone and account
  - Victim advocate should also delete all text messages
  - Survivor should be sure to use innocuous name in contacts for victim advocate so victim advocate's name does not show up when text alert comes in

Newer technology: Email

- Like texts, emails can be sent and received silently, so survivor may prefer to use it rather than be overheard on phone
- Like texts, emails create records of content of communication, as well as time-date stamp and even computer from which it was sent
- If using email, use the following protocols:
  - Both survivor and victim advocate should delete all emails to each other as soon as communication ends
  - Survivor should make sure email access requires two-factor authentication
  - Survivor should consider creating new email account not known to abuser and use that account on a different computer if possible
  - Send links to documents to survivor rather than attachments, so you can delete them if you know abuser has gained access to email

Newer technology: Chat

- Like texts and email, chat is a way to communicate with a survivor who does not want to be overheard while sheltering in place
- Chat originates from the organization that installs it on its server. If your organization has a chat function on your website, then the records will remain on your organization's side of the communication. Once the survivor closes the chat window, the record is gone from the survivor's phone or computer.
- Because the chat remains on your organization's server, you should have software that "dumps" the chat record as soon as the chat ends, so that you don't retain a record of the content of the chat or the URL the survivor was using to communicate with you.
- Chat leaves less of a record on the survivor's end
- The problem is that chat engages randomly with a victim advocate who is on duty. The survivor cannot ask to chat with a specific victim advocate
- Chat is good for helplines

Newer technology: Videoconference

- COVID-19 has introduced all of us to Zoom and other videoconference services
- Videoconferencing is helpful for group communications, such as outreach or education efforts
- It is also helpful for sharing documents or videos to others
- Depending on the version of the videoconference technology you use, you can use a password to ensure that only approved participants can join a videoconference
- Even where you use a password, it is always possible that it has been forwarded or shared with someone you did not want to attend
- Zoom now offers encrypted communications
- Though some now use videoconferencing for telemedicine and sometimes counseling, it is not the best technology for working remotely with survivors sheltering in place with their abusers

Safety Planning with Survivors

IF SAFE TO DO SO: call 911

Use Emergency SOS on iPhone https://support.apple.com/en-us/HT208076

Use emergency location sharing on Androids and iPhones

https://www.theverge.com/2019/3/18/18267500/how-to-set-up-emergency-location-sharing-android-ios

QUESTIONS?

Thank you!

robvalente@dvpolicy.com