Best Practices on Faxing

Despite the many ways technology allows us to communicate nowadays, the fax machine is still used by many programs. Although the basic use, sending and receiving documents, hasn’t changed much, how the technology works has evolved. Depending on the type of fax you use, the information you share could be vulnerable to interception or access by others. It is quite easy to accidently access faxed communication if safety and privacy protocols aren’t in place.

**Traditional Fax Machine**
Traditional faxes use a phone line to send and receive information. Risks for this type of faxing depend on who picks up the fax at the receiving end. If you’re sending it to an office, your fax could be piling up along with all the other faxes they receive.

**All-In-One Fax, Scanner, Copier Machine**
Many fax machines are now multipurpose and users can send faxes as well as scan and print documents. These machines often have hard drives that retain a copy of every fax received, scanned, or printed. For this reason, if your agency sells your fax/copier machine or the lease on it ends, it is important that you retain the hard drive and destroy it. Otherwise, all the sensitive documents you’ve ever received, printed, or scanned could be available to the new owner of your fax/copier machine simply by pulling it from the memory. (Some machines have additional security and will wipe the hard drive regularly; check to see if this is an option on your fax machine but keep in mind that this may be an added expense.)

**E-Fax**
Another way to fax documents is through the internet without needing a fax machine at all. These services can send faxes to and from any device that has internet access, such as your smart phone, tablet, laptop, or computer. If sent to a device other than an actual fax machine, the information will come in the form of an email. Documents that are received via email can be vulnerable to access, either by anyone who has access to that account or by interception. Moreover, unless you delete the email and attachments from your inbox, deleted folder, server and backups, it could be possible that you will retain that information or document longer than you want.
Survivor Risks and Vulnerabilities
Faxes are often used when agencies want to transmit documentation for or on behalf of survivors. This documentation can contain sensitive or personal information; if intercepted or accessed, it could violate the survivor’s privacy. Moreover, be aware that even the fax number could reveal a survivor’s location, creating an increased safety risk.

Best Practices When Faxing
Talk to survivors about the possible risks of utilizing fax services and safety plan accordingly. They should be aware that it may be possible for someone to trace the original fax phone number and could locate them.

Be cautious about using public faxes or faxing services available at stores if sending sensitive information. That information may be stored in the hard drive of the machine.

If you are forwarding a fax message to another agency, make sure that any identifying information (usually located at the top) is cut off of the page from the original fax.

Before you send a fax, call to make sure that the person the fax is intended for will be there to pick it up.

If leasing a machine, negotiate the contract to ensure that your agency can keep the hard drive at the end of the lease period to maintain control over the data. Alternatively, ask for a machine with additional security options, such as pass coded access a hard drive that periodically purges data.

If you donate, sell, or end the lease of your fax machine, take out the hard drive or work with your vendor to shred the information storage device within the machine so the next owner doesn’t have access to your information.

If you are sharing a fax machine with other agencies, the machine should be in a secure area with strict policy on access and usage. Consider using personal passcodes in order to access faxed and printed documents. Advocates and programs that have strong confidentiality obligations should not share a fax machine with other programs that may have weaker confidentiality
privilege or obligations.

Have retention policies around emails so that faxed communications that are received via email aren’t kept longer than intended.

When using e-faxing services, you may need to check with the receiver of the information to make sure all pages were transmitted. Unlike a traditional fax machine, e-faxing does not track and record each page sent. Because of various transmission practices, it is possible the fax is not received instantaneously. Fax services (like E-Fax, MyFax) often keep logs and records of documents and corresponding information sent and received. It is important to carefully read the privacy, retention, and access policies of the service provider so that you understand the limits of their protections.

©2014 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVC Grant # 2011-VF-GX-K016. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.