Record Retention and Deletion

Why should we have record retention and deletion policies?

- A survivor's data belongs to the survivor; agencies might collect and store a survivor's data temporarily in order to better support that survivor's needs, but if your agency or collaboration collects data, it has an obligation to safeguard that data, and make sure that your data collection activities do no harm.
- Any data collection or sharing you undertake should result in decreased risks to victims; your data collection processes should never increase risks for victims.
- Some agencies and coordinated community responses (i.e., with courts, law enforcement, prosecutors) have practices or obligatory situations where they might share a survivor's data or make it part of a public record or online database. For safety reasons, any agency or partnership that has these practices or obligations should provide upfront notice to the survivor and fully discuss all options a survivor has to prevent or restrict the data access or sharing including sealing or restricting access to a record, and, preventing a record from being published online for safety reasons.
- As part of any data collection activities, it is better to have accurate data. Because victims' lives and circumstances change, especially when having to respond to the perpetrator's tactics, the data an agency collects one day can become outdated or inaccurate tomorrow.
- Programs get requests for survivor data all the time. While most programs cannot respond by sharing identifying information unless the request is a court order or a mandate by state law, programs should still work to minimize the amount of information that is maintained by the program. If the information doesn't exist, it cannot be a privacy risk for the survivor.

To increase victim safety and record accuracy, you should have clear policies and processes at the program, agency, and collaboration level that address record review, retention and deletion.

Why is it best practice to collect minimal information?

The more client data you collect, the greater the confidentiality risks to victims and the more steps your agency will need to take to protect that larger amount of data. When creating policies that address how long to keep agency records, it's important to first examine what data is being collected and its purpose. If a primary goal of your services is to support survivor safety and confidentiality, then your agency should make sure that you never collect or retain data that could inadvertently harm or increase risks for a survivor. For example, sometimes, a perpetrator's lawyer will to try to access records about survivors from shelters, rape crisis centers, Family Justice Centers, and other service providers.

The best practice to follow for data collection is to collect the minimum amount of information needed by your agency to provide services. It is best to stick to the facts; detailed case notes or narratives

This project was supported by Grant No. 2007-TA-AX-K012 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

describing full conversations with a survivor are often unnecessary. Agencies should refrain from including subjective assessments of the victim by agency staff. Additionally, a survivor might feel comfortable telling an individual staff person about information not related to the present violence she is experiencing, such as being a child abuse survivor or having a health disability; yet it might not be relevant or helpful to the survivor to document those sorts of details in your intake form or record. As part of informed consent, it is best practice to be transparent and to ask the victim what information s/he does or does not want included in intake or other agency forms.

Why is it best practice to collect a range of data, not specifically identifying information?

Another best practice is to collect information in categories, such as asking survivors to select an age range rather than provide a date of birth, since it is less personally identifying.

How long should a program keep records?

The length of time that specific records are kept may depend on who is collecting the information and the types of services provided.

It is important to fully understand how your state's or territory's record retention laws or licensure regulations apply to individual staff within the agency. Some licensed practitioners, such as therapists, attorneys, and counselors, may be required by law to keep certain types of files for a certain number of years. It is important to find out whether or not the regulations apply to the licensed practitioner regardless of where and when they are working; if so they might apply to that licensed practitioner when they are working within your agency or partnership. Otherwise, some regulations only apply to the licensed professional when working in a specific capacity or setting. The law or regulation may also define what type of information needs to be retained. In this case, it is best practice to retain the minimum information deemed necessary by that law or regulation and to purge anything else. If you are unsure, you can always ask the victim what information they think is necessary for your agency to keep. A good thing to consider including in your agency policy are practices where you regularly ask victims about their data records: let them review the records, tell you what is outdated, and, what information they want removed or kept for safety or privacy reasons, and what information may or may not be shared in the case of death and a fatality review. Additionally, if a licensed practitioner does need to keep detailed records for a certain number of years, it is important to assess whether that practitioner should keep those files separate and segregated from the agency's other files and records. In any such privacy and risk assessment, it is good to review the implications for victim safety and confidentiality by exploring the wide range of scenarios that might impact victims.

Who should have access to the data?

Data retention policies should include a process for identifying and setting access levels. Because data collected in programs is confidential and contains sensitive information of individual survivors, agencies should establish who can have access and view that data. For example, the database can be set up so that a volunteer, intern, or certain staff who do not work directly with survivors can only pull aggregate data (i.e., how many people were served with a particular service within a time period)

This project was supported by Grant No. 2007-TA-AX-K012 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

rather than individually identifying information. Just like some paper records are kept locked up with only senior staff having access, access levels on data being retained in databases helps maintain confidentiality.

Are there special precautions our agency should take to protect records until they can be destroyed?

Older records should have the same level of protection as current records. To maintain your confidentiality obligations and protect safety and privacy, both paper and electronic records should be kept secure. Data collected in programs is confidential and contains sensitive information of individual survivors. Thus, agencies must set boundaries on who can access and view what data.

Paper: It is not considered best practice to store older paper records by simply boxing them up and stacking them in a storage room that all staff can access. Paper records should be kept locked up with clear policies about which staff can access what records under what circumstances. If paper records are stored in boxes, label and date the boxes and files clearly and prioritize confidentiality when deciding how to group records per box.

Databases: Access levels to databases should be similarly restricted to the staff necessary to complete the job role. For example, the database can be set up so that a volunteer, intern, or certain staff who do not work directly with survivors can only pull aggregate data (i.e., how many people were served with a particular service within a time period) rather than individually identifying information. It is best practice for each person working for the agency to receive a unique user name and password with appropriately restricted access levels for their job role. When an individual leaves the agency, their unique user names and passwords should be immediately deactivated or deleted so they can no longer access the database, or any computers and devices that are set up to access the data or database such as servers, desktop and laptop computers, USB storage devices, smart phones, ipads and tablets.

Why should your agency purge data regularly?

When record retention lengths are not mandated by any law or licensure regulation, it is best practice to have a policy of purging records regularly to delete any detailed information that is no longer needed. Survivors lives and circumstances change. Purging data regularly protects their confidentiality and ensures that you are not retaining or acting upon outdated or inaccurate information. For example, when a victim first comes to shelter, you may need to document what s/he requests, such as housing or counseling or other specific requests. After the survivor leaves shelter, all you may need is a record that services were provided by the program. Purging detailed information in records could be done every 3 months or whenever a survivor leaves the program. Again, if minimal information is collected in the first place, purging unnecessary information from the file later will be easier.

Do financial records have to be retained for a different amount of time than counseling records or client files?

Possibly. The financial and billing records for your agency may need to be kept for a different amount of time for the U.S. International Revenue Service (IRS), tax regulations, or for audits by grant funders.

This project was supported by Grant No. 2007-TA-AX-K012 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

Make sure you understand all applicable rules. Again, it is best practice to ask the relevant agency that conducts audits and consult with an attorney familiar with your jurisdiction's laws and regulations.

What about other types of records, such as security or surveillance videos?

Any time that security or surveillance videos are used, survivors or anyone entering your facility should be informed that they are being recorded. Many times this is done through visible signs that state that security cameras are in use.

In terms of retention, your agency should have a policy stating that surveillance video records are purged on a regular basis and should detail any exceptions to this policy. Examples of exceptions might be when a video camera records an abuser violating a restraining order, or some other record of a crime. Clients should be notified about these exceptions. Since surveillance cameras are usually used in case of emergencies, purging every 24 or 48 hours is suggested.

We always shred our paper files before disposing of them. How do we ensure our electronic files are "disposed" of in a secure way?

First, an agency needs to understand and map all the places where copies of their electronic files may reside including: desktop computers, laptops, servers, back up discs and services, email accounts, databases, internet service providers, phone providers, phones, TTY and fax machines, printers and photocopiers. For example, like computers, most fax machines, photocopiers, and networked printers also have hard drives inside them that should be fully cleaned before being returned to the rental company or resold. To ensure that the data on a hard drive is not recoverable, it is not enough to simply delete the files or reformat the hard drive. Instead, best practice is to either physically destroy the hard drive platters with a hammer or to use a software program that overwrites data on the drive to NIST standards.

If your agency is not vigilant about destroying electronic files, and someone else later gets access to the device and retrieves your confidential client data, it might have a harmful impact on survivors and your agency might be held liable.

Overall, what data retention policies should our agency have?

Your agency's data retention policies should coexist seamlessly with your agency's data collection policies and at a minimum cover:

- What records you collect related to a victim (and related children).
- Why you collect the records that you do. Demonstrate a clear need or rationale.
- How records such as intakes and case notes are kept.
- What type of data is entered into any file or database (e.g. date of birth versus age range)
- What the process is for consenting to or opting out of being entered into a database or file.
- How someone can request to see or request edits to a record about them.
- The length of time specific records will be kept.

This project was supported by Grant No. 2007-TA-AX-K012 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

- The process for purging data, including how paper and electronic data are securely destroyed, and, how and when inaccurate and outdated data gets automatically or manually deleted.
- What data will be purged versus what data will remain and for how long (time frames).
- How records are separated or restricted to address privilege or licensure record retention laws or regulations.
- Which types of records your record retention policy pertains to.
- Access levels: who can access what data, and how access is changed or revoked.
- How any records you retain are stored securely until they are destroyed.

This project was supported by Grant No. 2007-TA-AX-K012 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.