The President's Family Justice Center Initiative

Confidentiality, Information Sharing, and Privacy Protocol Recommendations

August 2005

Prepared by the National Network to End Domestic Violence, the San Diego Family Justice Center Foundation, and the Office on Violence Against Women of the United States Department of Justice

Table of Contents

Introduction

This policy document is intended to represent a set of guiding principles and recommendations regarding confidentiality, information sharing, and privacy policies and procedures implemented at any Family Justice Center (FJC) funded through the President's Family Justice Center Initiative. The Safety Net Team of the National Network to End Domestic Violence (NNEDV) is the primary author of this document though not all recommendations contained in this document are supported by NNEDV. The San Diego Family Justice Center Foundation Comprehensive Technical Assistance Program Team (SDCTAP) has also assisted in preparing this document though SDCTAP does not support all recommendations made in this document. SDCTAP and NNEDV, on certain matters, have different philosophical views related to confidentiality, information sharing, and client privacy. Where possible, the positions of NNEDV and SDCTAP are identified, particularly if such recommendations differ. Each FJC community should carefully consider the differing views in reaching their own consensus on the appropriate approach for their particular FJC.

NNEDV has a strong commitment to complete confidentiality with all client information at a FJC. This commitment extends to NNEDV's position that identifying client information should not be maintained in a central FJC system but rather by individual partner agencies, that services should be provided anonymously to clients if so requested, and that sensitive fields within client records should be purged regularly to protect the confidentiality of clients. SDCTAP, on the other hand, maintains identifying information on all clients at the San Diego Family Justice Center and does not support eliminating identifying records or allowing clients to remain anonymous at any time during the provision of services at a FJC. SDCTAP supports maintaining client demographic information in perpetuity while making every effort to keep such information confidential. All sites should review state law on records retention to ensure compliance including prohibitions on the destruction of records by public agencies.

Working collaboratively, NNEDV and SDCTAP have prepared a document that notes differing recommendations from NNEDV and SDCTAP in certain matters, and anticipates each federally funded FJC will evaluate the complex issues involved in creating policies and procedures for operation. The overriding theme of all policies recommended in this document, however, is support for protecting the confidentiality of client information at a FJC. In the absence of client authorization, information gathered from any FJC partner should not be shared with any other FJC partner. NNEDV and SDCTAP also concur that all client information at a FJC should be protected from all disclosure to outside sources to the greatest extent possible under local, state, or federal laws and policies.

Each FJC in the President's Initiative is developing their own policies and procedures related to confidentiality, information sharing, and client privacy. This document is intended to assist each Center in evaluating the many critical issues and developing written policies and procedures that will guide operation of the Center and address all relevant matters related to confidentiality, information sharing, and client privacy.

Essential Considerations

- Confidentiality is critical to safety and encourages help-seeking by victims.
- Not following practices that protect confidentiality can lead to civil or even criminal liability.
- State laws vary and must be followed by the FJC and its partners.
- FJC clients/victims have the right to know what will happen to their information.
- The FJC and its partners should err on the side of protecting confidential information and should resist disclosure by all appropriate means.
- Client identifying information obtained and maintained should be the absolute minimum necessary to provide services.

General Philosophy and Principles

The FJC and all partner agencies should recognize that the goal of the FJC is to provide access to domestic violence victim services that enhance victim safety. Victim safety can be compromised by the failure to maintain the confidentiality of client information. Conversely, when authorized by a victim, information sharing may increase the effectiveness of service delivery and increase victim safety and abuser accountability. The FJC, and all of its governmental and non-governmental partners, should affirm that confidentiality and privacy protections are critical to serving victims/clients who use the FJC and should not share information in the absence of client authorization.

The FJC, and all of its governmental and non-governmental partners, should recognize that victims/clients retain the right at all stages to choose what personal information to share with the FJC and its individual partner agencies, including the choice of who within and without the FJC and its partners may have access to the information.

The FJC and its partners recognize that the FJC itself, and the various partners who are collaborating through the FJC, may each have different obligations concerning confidentiality of victim/client information. The FJC should recognize that those individual, professional confidentiality obligations continue, and must be honored within the entire FJC collaboration.

It should be the policy of the FJC and its partners to hold confidential, to the extent possible under state and federal law and policy, all communications, observations and information made by or about victims/clients.

- The collaboration of the partners through the FJC does not limit or eliminate confidentiality protections for victims/clients, but requires constant vigilance in order to ensure that confidentiality of victim/client information is protected.

- "Confidentiality walls" are needed to protect confidential information and preserve the integrity of the FJC collaboration. Such "walls" may be needed both within the FJC to protect confidential information that a victim/client or a specified professional has, and to protect the confidentiality of FJC victim/client and professional information from requests for information from outside the FJC.

- Staff, volunteers, counselors, advocates, board members, student interns, consultants, independent contractors, and other community partners at the FJC should understand that their continued employment or volunteer position is contingent on adherence to all privacy, information sharing, and confidentiality policies. The FJC will provide a legal defense to any staff person or volunteer who is subject to lawsuit because of their compliance with adopted confidentiality, information sharing, and privacy policies.

- All staff, volunteers, counselors, advocates, board members, student interns, consultants, independent contractors, and community partners must sign a written agreement to comply with all privacy, information sharing, and confidentiality policies. This agreement should be placed in the personnel files of the staff and in the individual files of volunteers, counselors, advocates, board members, student interns, consultants, independent contractors, and other community partners at the FJC.

- All victim/clients must be provided information about the Center's confidentiality policy and practices, and their rights under such policies.

- The obligation to maintain confidentiality does not end when the service to a victim/client is concluded. Confidentiality extends to all current and former victims/clients.

- The FJC and each partner should follow all relevant laws and policies related to confidentiality, information sharing, and privacy of victim/client information. In the event that there is a dispute or disagreement about whether victim/client information should be protected from disclosure, the FJC should err on the side of protecting the information and should resist disclosure by all appropriate means.

Family Justice Center Internal Confidentiality Protocol

Note: These recommendations are designed to be the basis for protocols for the FJC on-site partners. Off-site partners should be required to adhere to the general principles set forth above, to collaborate in the confidentiality audit process as requested, and to develop their own confidentiality protocol that is consistent with this Family Justice Center Internal Confidentiality Protocol.

Managing confidentiality of information inflow

Information that victim/clients share with a FJC is confidential, including personal identifying information such as name, address, and phone number, subject only to a victim/client's specific, informed, written, consent for release or sharing of confidential information, [See Appendix E. Limited Release of Information Form] and mandatory medical or child abuse and neglect reporting requirements. To best protect confidentiality, a FJC should have its central intake staffed by domestic violence advocates whose communications may be protected by local, state, and federal confidentiality laws and policies. *Note: If there are other exceptions under specific state law, protocols prepared consistent with this document should be included in each site's completed policy documents.*

Information that comes in to the FJC from victim/clients is confidential, including identifying information. The FJC is charged with protecting that information as required by law.

Information about a victim/client that is provided to the FJC from another confidential source should also be subject to the confidentiality protections set out in this protocol. The procedures below should be considered for protecting confidentiality of victim/client information that is created and maintained in a FJC:

Building Security Desk information

If there is separate building security, separate from FJC check in processes, Centers should consider the following protocol provisions:

- If visitor or appointment logs are kept at a building main entrance, the information collected in the logs should be voluntary and optional.
- If a victim refuses to give their name, they should not be denied access by building security. Someone affiliated with the FJC should determine if a person is eligible for services at the FJC.
- If visitor badges or nametags that identify a victim/client are offered, their use should be voluntary and optional, and the victim should be advised as such. Victim/clients should not be required by FJC building security staff to give their full name to access the FJC.
- Victims/clients should be told they have the option to use only first name or any alternate name.

Why purge the security logs?

If the FJC is located in a place where those who enter the location can be identified as a client or potential client of the FJC, there is a potential for breach of confidentiality, and a risk of liability. Purging the logs and other records on a reasonable, but short, time frame will help protect confidentiality while providing information necessary for security if needed.

Which time frame makes sense for our FJC?

The suggested 24/48/72 hour times for purging security information are designed to balance the need for confidentiality of the client/victims who use a particular FJC and the need for security if a security breach occurs. For example, if an assailant enters the FJC and threatens his partner or staff, the surveillance video could be useful evidence. The time frame should be the shortest amount of time necessary to ensure that the video can be preserved if a security breach occurs.

Information Collected During the FJC Intake Process

Because information collected through centralized intake systems is inherently more vulnerable to security risks, FJC staff and volunteers should collect minimal central demographic information and information regarding what services the victim/client requests and uses.

> Minimum central demographic information includes gender, age, ethnicity, number of children present, types of services requested, and types of services provided.

If the FJC central intake system collects information that could identify individual victims, it should be the policy of the FJC that regular audit data trails will be performed to examine data queried and user access.

> **Will the general, non-identifying data be sufficient to demonstrate to FJC funders that the services have been provided?**
>
> Yes. OVW and the other federal partners don't need to know the identities or the names of clients who receive services. Although certain client-level identifying information may be purged to increase victim confidentiality, for audit purposes, the FJC must have a record of payments that were made and services

It should be the policy of the FJC to allow all victim/clients upon request to review their identifying information. Victims should be informed about security and data sharing policies. They should be informed about the process to inspect or correct their data/records. NNEDV recommends that clients be allowed to opt out of providing identifiable information and that clients be allowed to edit or remove their identifying information. SDCTAP recommends an FJC maintain all such information under its control and that clients not be allowed to remove identifying information or opt out of such information collection. SDCTAP recommends collecting identifying information on all clients but concurs that all such records should be maintained on a confidential basis.

The FJC staff or volunteers working at the FJC front desk/intake process should not record intimate details of a victim/client's life story in any central files or records. If victim/clients share more information than requested, staff and volunteers should not document this information in any central FJC electronic or paper files.

> Different professionals within the FJC have different levels of confidentiality and privilege. The professionals who have greater privilege may obtain more detailed information from a victim/client, but if that professional shares the information with another partner through a database or otherwise, the privilege might be voided.

Intake, Assessing Interest in Services, and Safety Planning

All FJCs should identify which partner organizations and staff roles are required by law to maintain confidentiality and/or privileged communications with victim/clients, and the extent of such confidentiality and privilege protections.

If the FJC has the capacity to immediately assign an advocate required by law to maintain confidential and/or privileged communications with victim/clients, that advocate may conduct a more thorough and personal assessment with a victim/client about services needs. Regardless of whether or not a more extensive intake conversation takes place, the information documented in FJC central files should remain limited to only demographics and services requested. It is recommended that the only instance where more extensive intake information might be documented is by an advocate for an individual partner agency that remains protected by that advocacy agency's confidentiality policies and practices, unless the client has authorized the sharing of information between partner agencies at the FJC.

Victim/clients should be able opt-out of having their information recorded in a computer. If victim/clients choose not to have their information recorded electronically, they should still be provided services and paper materials only should be maintained by the FJC.

Victim/clients should be informed prior to any audio or videotaping of their conversations with staff or volunteers of the FJC and its partner agencies and should be offered the option to opt out of participating in any such recorded conversations.

We record conversations for security and teaching purposes. Can we still do that?

The FJC is encouraged to evaluate the confidentiality risks relative to the purposes and benefits of recording such conversations. The FJC should also determine whether to keep such recordings in a way that links it to a particular client if the purpose of the recording (such as teaching) can be met without identifying the client. Certainly, if recording is proposed, the victim/client should be provided with complete information about the access, storage and use of such recording, and her rights to review and remove such information from her records, and ought to provide written consent to such recording.

Protecting confidentiality while collecting victim information

Computer monitors should be arranged to prevent members of the community, victims, and others from accidentally or intentionally viewing other victim/client confidential information on FJC and its partner's computer screens. Password-protected screen savers can be used as an added layer of security whenever users leave their desks. For example, if a hospital or other landlord has donated space to an FJC, landlord employees that are not part of the FJC should have clearly physically divided space from the FJC, including walls and doors with locks that allow both parties to completely physically separate themselves from each other.

Example: if the hospital has donated space to a FJC, hospital employees who are not part of the FJC should have clearly physically divided space from the FJC, including walls and doors with locks that allow hospital employees to completely physically separate themselves from the FJC employees. Doing so will help protect victim/client confidentiality and patient confidentiality.

There should be a clear physical separation between the FJC administrative process and any entity which has donated or rented space to the FJC. If other entities have physical access to the FJC, the FJC should clearly document how paper records, computer records, and all other victim information will be protected.

Managing confidentiality of information maintained by the FJC

The procedures below should be considered to protect confidentiality of victim/client information that is held by the FJC:

Protecting any information collected by the FJC

A FJC may implement a limited central intake system using either paper or a combination of paper and electronic intake forms. Victims/clients should be informed of their option to bypass the FJC central intake system and of their right to provide intake information on paper. While different Family Justice Centers may handle such procedures differently, all Centers should consider creation of an "opt out" process for clients that do not want their information electronically maintained. NNEDV further recommends that clients be allowed to receive anonymous services if they so request. SDCTAP supports this recommendation only in unique and limited circumstances as determined by the FJC. SDCTAP otherwise recommends that all clients be required to provide identifying information in order to conduct a limited background check to ensure the safety of all other clients at the FJC in the event a potential client has a criminal history or is otherwise a security risk.

If any computer used to access a FJC limited central intake system also has Internet access, then no more than the victim's/client's first name or pseudonym should be entered in this central intake system. If this intake system is on computers that are networked with shared electronic networks or other entities, these computers should have strong security protections.

NNEDV recommends that if a victim's/client's name is included in the FJC central intake, it must be voluntary, pseudonyms should be allowed, and full names should be purged (choose one) before midnight or within 24 hours. NNEDV recommends that a victim's name should not be attached to a victim's/client's file beyond that particular FJC visit. NNEDV recommends that names should simply be used to make their visit that day more personal. SDCTAP recommends maintaining all such records, including full names and identifying information, opposes purging of information, but supports enforceable confidentiality policies with all such client information. SDCTAP supports maintaining a victim's name with the client file beyond a particular client visit.

NNEDV Position: Programs are encouraged to keep names or specific identifiers out of the central database, but if strongly desired, names could be kept on paper for 90 days, and cross-referenced with an assigned ID number. For a limited time period, limited FJC staff could check to see whether or not a client was at the FJC previously and connect them to the partners they visited previously. But with the list, it is time-limited, and lessens the risk of disclosure through the computer data base.

Securing paper and electronic information

Security measures should be in place to protect all electronic and paper records. Paper should be stored in locked filing cabinets in locked rooms. Electronic records should be properly secured electronically, with alpha-numeric passwords, and where appropriate, user access levels that are limited to the minimum access level necessary to perform a job role. NNEDV recommends that if electronic backups or paper copies of the central FJC intake records are stored off site, they should be protected and purged in the same manner and within the same time limits as information stored onsite.

If a FJC chooses to have an electronic limited intake system, and a user forgets a password, the user should (select 1 or more options)

- Use paper files until they are able to reach the system administrator for a new password;
- Log in with the permission of another user with a similar access level under that user's account, carefully document the anomaly, and then have both users' passwords changed within (select option) 12/24 hours or as soon as they are able to reach the system administrator;
- Contact the on-call system administrator (if the FJC has one).

Managing confidentiality of information outflow

The procedures below are recommendations for protecting confidentiality of victim/client information that is requested from the FJC by its partners: (also see section III)

- In order for confidential victim/client information to be shared between the FJC and one or more partner or non-partner agencies, the victim/client whose information is sought must be informed of the implications of sharing that information to the fullest extent known, and should voluntarily consent by signing a limited release of information form, in order to provide the highest level of confidentiality protection possible for FJC victim/clients.

- NNEDV recommends a Limited Release Form that authorizes information sharing for only a limited time period and allows for verbal withdrawal of consent by the client even after authorized release. SDCTAP does not recommend such limited, specific release forms. SDCTAP recommends a general release form after an informed consent process. Samples of both types of forms are included in the Appendix of this policy document.

The FJC should only share confidential information about an individual victim/client with partners upon the signed written request of that victim/client.

Release forms from other agencies, or forms that contain blank lines should not be accepted. Victim/clients should meet with appropriate FJC staff or volunteers to be provided with the information needed to provide knowing consent to the release of information. Any blank lines must be "X'd" out before the victim/client signs any release. Release forms should be signed and dated in ink.

Limited sharing of FJC intake information with FJC partners

If information is going to be shared, the FJC central intake system should function as a one-directional system, with information shared only to agencies chosen by the victim. Information from the chosen agencies should not be sent back to the intake database or shared between additional agencies without the explicit time-limited consent of the client.

A victim/client may request that any information already completed on paper be copied so that the victim can choose to provide paper copies to partner agencies.

If a victim would like only limited intake information shared with one or more partner agencies, the individual partners should not be told about other partners the victim is choosing to access, but only the limited demographic information, unless authorized by the client.

Limiting access to central FJC information

With the exception of individuals who are responsible for staffing a FJC front desk and any associated central intake processes, the staff of partner agencies should not have general access to FJC central intake records with names attached to them, unless authorized by the client.

Since even demographic data can be identifying if someone knows the date of visit and demographic details of a victim, the central intake system should have limited access. If the FJC allows partner agencies and other non-intake staff or volunteers to access the FJC central intake system, the data system should have an audit trail that records all access and queries of the central system by individual users.

An audit trail can provide information about who has used the system and for what purposes, in addition to how well confidentiality protocols are being followed.

The procedures below are recommendations for ways to protect confidentiality of victim/client information that is requested from the FJC by non-partners:

Confidential victim/client information should not be provided by the FJC to any non-partner, except that non-identifying demographic information may be provided to evaluators and auditors to evaluate the effectiveness of the FJC.

If any victim/client referrals to non-partner service providers are warranted, such referrals should be made in such a way as to preserve confidential victim/client information.

NNEDV Position:
Referrals to non-partner providers can be made in a way that preserves confidentiality by giving the agency information to the client so she can contact the agency directly.

Partner Internal Confidentiality Protocols

Managing confidentiality of information inflow

Confidential client information that is provided to the partner by the client directly should be confidential if the partner has confidentiality protection (such as clergy, attorney, domestic violence advocacy agency, therapist, or physician). Confidential communication that is received by the partner from the client should not be shared with the FJC by the partner, except for limited, non-identifying demographic information for evaluation and auditing purposes, unless specifically authorized by the client and based on informed consent. When possible, this information should be provided in aggregate formats.

As part of a commitment to supporting a victim's/client's right to informed consent, FJCs are strongly encouraged to collect and learn about the confidentiality and privilege policies of all of its partners and provide basic information to victims/clients about the confidentiality options associated with individual partner's services.

The procedures below are suggestions for practices that can help to protect the confidentiality of victim/client information that is provided to a FJC partner:

Maintaining the confidentiality of incoming faxes

Partners with confidentiality or privilege protections must make all attempts to have their own fax machines for incoming faxes.

Other partners should ask those who are faxing victim related information to call ahead of time so the FJC partners can make a reasonable attempt to remove them promptly from a central fax machine. If the shared fax machine used for receiving non-confidential information saves scanned information to a hard disk, the FJC should attempt to continually overwrite the memory of any central fax machine.

Each FJC is encouraged to protect victim/client confidentiality by not using email-based faxing for any community partners, volunteers, or staff to receive confidential victim/client data or records.

Responding safely to possible incoming requests for assistance from email and websites

If the FJC or partners have websites that provide an online mechanism for contacting the FJC or publishing partner email addresses, the website should include safety tips for victims including at least the following information:

- External email coming from a FJC web form provides a victim (or other website visitor) the ability to share the safest way to reply and the opportunity to complete a brief online "safety plan".
- When responding to survivors, it may be best to delete the entire original message (do not include the original message in the reply), in case others read the response.
- Partners may choose to create and include a brief sentence about email privacy and safety issues at the top or within the signature/footer of some or all outgoing emails.
- Staff or email accounts that receive external emails from survivors, might choose not to use auto-response emails when they are out of office.

Protecting confidentiality while collecting client information

Anyone with privilege or confidentiality protections should have a walled office with a door or use a private and closed office to meet with clients and have confidential phone calls.

If FJC partners meet with victims in offices with windows opening into hallways or to the outside, partners should attempt to use blinds or other coverings to protect identity of victims within the office if the victim/clients can otherwise been seen.

If computers contain sensitive client information, the monitors should be turned so that people walking by cannot see confidential information. If victim information is typed into a computer while the victim is present, staff should make an attempt to turn the monitor so that victims can see anything being entered about themselves.

Partners entering victim information into computers should use password-protected screen savers to protect confidential information if they walk away from the computer.

Examples of ways to protect confidential client information:

1. Use walls or screens for privacy;
2. Have separate fax and phone lines;
3. Have computers that are password protected;
4. Turn computer monitors away from possible public view.

Managing confidentiality of information maintained by each FJC partner

The procedures below are requirements for protecting confidentiality of victim/client information that is maintained by the FJC by partners. Partners that have a confidential relationship with a victim/client (e.g., clergy, attorney, domestic violence advocacy agency, therapist, or physician) must have a protocol for maintaining and destroying confidential victim/client information.

Securing paper and electronic information

It should be the policy of the FJC that all onsite community partners will have locked filing cabinets kept in locked rooms to house all paper copies of victim/client records. Clearly defined access levels should identify who has access to the keys for the filing cabinets, storage rooms, and offices. FJC staff, volunteers, and all community partners should follow strict procedures for securing all keys for filing cabinets, storage rooms, desks, and offices.

Who owns the file cabinet and who owns the files? And who owns the hard drive, and who owns the data?

Ownership of the storage location doesn't mean ownership of the items stored. For example, the FJC might own the file cabinets, but the files may be owned and managed by the community partners. Under this recommended policy, external hard drives are considered to be owned by the program that owns the data.

It should be the policy of the FJC that all community onsite and offsite partners will retain ownership of all data and their victim/client records. The FJC and other community partners must honor individual professional confidentiality obligations as established by federal law, state law, and policies. It should be the policy of the FJC that all community partners including attorneys, advocates, and counselors will own their own computer hard drives, external drives, or any other electronic media.

Since community partners own any external hard drive used to store records, files or documents, community partners are responsible for maintaining secure backups of that data.

Partners should determine how much identifying victim information is appropriate and necessary to collect, and attempt to minimize the amount of sensitive or identifying information collected whenever possible. NNEDV recommends that all community partners at a FJC remove identifying or sensitive information as soon as the information has served its purpose. SDCTAP does not concur in this recommendation and instead recommends maintaining all information in a secure system, for a period of four years.

If the FJC owns the computer that any FJC partner uses to house victim information, the FJC partner should still maintain ownership of and retain all data on the hard drive. If the partner organization is no longer affiliated with the FJC, the partner should take the hard drive with them and the FJC should replace the hard drive.

Hard drives containing victim information should not be given to any other organization, thrown away, or given to another partner until the data has been destroyed through complex computer wiping programs where all data is written over, or by physically destroying or shredding the hard drive. Using a Windows "High Level Reformat" is not a secure means to destroy confidential victim data.

If the partner keeps confidential records onsite, each partner should have a locked filing cabinet or safe to house paper copies of victim records and removable hard drives if used. Keys will be secured and access to these locked spaces should be limited.

If a partner chooses to have email or internet access on a free-standing computer containing victim information (not networked to other partners or entities), then the partner should be responsible for installing and maintaining firewall(s), anti-virus software and implementing all reasonable computer security measures.

Users who have advocate, counselor, or attorney privilege should not share their computer(s) with others who are not protected by the same organization's confidentiality or privilege protections.

Maintaining confidentiality if FJC uses shared electronic networks

If the FJC owns the computers and network and provides all networking, then partners with confidential information should make every attempt to save confidential data to external hard drives. Partner computers can be set to not allow information to be saved to the "C drive" or any network drives, so that all victim information is saved to an external drive. Partners should be responsible for backing up their own data.

It should be the policy of the FJC that all computers with Internet access or those networked to others with Internet access will be secured with firewalls and updated virus protection.

Managing confidentiality of information outflow

The procedures below are recommendations for protecting confidentiality of victim/client information that is requested from the FJC partners by any other agency, including the FJC itself:

Whenever confidential victim/client information is sought to be shared between the FJC and any partner or non-partner agency, an informed release by the victim/client whose information is sought to be shared should be required. SDCTAP recommends one initial general Consent/Release Form executed during the initial intake process. SDCTAP has found during three years of operating the San Diego Family Justice Center that information sharing among agencies is generally supported by victims and assists in providing effective services once authorized by the client. NNEDV recommends separate authorizations and specific, informed releases as necessary at varying times during the provision of services.

FJC partners should only share confidential information with other partners or non-partners upon the written authorization or executed release of the victim/client and based upon informed consent..

In order to provide the highest level of confidentiality protection possible, NNEDV recommends that the process should provide for a written release only upon informed consent that includes all of the following:

1. A review with the victim/client of the specific information that is to be released;
2. The risks and benefits of releasing the confidential information;
3. The reminder that the partner and the victim/client may not be able to control what happens to the information once it has been released to the outside agency, and any anticipated further disclosures that may occur (e.g., a release of therapy notes to a prosecutor may require such notes to be provided to the criminally charged perpetrator);
4. The purpose for which the information is to be released;
5. The duration for which the release is valid (choose one: 15 days/30 days);
6. The method by which the information will be released (e.g., phone call, copied documents sent by mail, e-mail, etc.) and the risks of such method of communication; and
7. Designate specific agencies or individuals to whom the information will be released.

NNEDV recommends that releases may be withdrawn at any time, and the withdrawal is effective as soon as it is given. Oral withdrawals are as effective as written withdrawals, although an oral withdrawal should be reduced to writing as soon as possible. SDCTAP does not support such on-going authority to withdrawal prior consent to release of confidential information nor does SDCTAP support verbal withdrawals of consent to the prior release of confidential information.

Using email and wireless phones for non-confidential communications

Partners should determine the appropriate use of wireless cell phones for use in communicating sensitive information, striving to not share identifying information about potential victims/survivors. On rare occasions when staff might need to use a cell phone to call a possible victim/survivor, staff should tell the person that they are using a cell phone and suggest that they not use last name or other very identifying details.

Staff discussing sensitive work information from a home phone should make every effort to use a traditional "corded" phone, rather than a cordless phone.

Whenever possible, FJC partners should not send or forward emails containing identifying information about a victim without first removing identifying details. Whenever possible, staff should attempt to assess risk and choose the safer methods to share potentially identifying and confidential information about possible victims.

Confidentiality Monitor Processes

The FJC and its partners should identify a "confidentiality monitor" whose job it is to review the partnership operation and identify areas where confidentiality can be strengthened. The responsibilities of the "confidentiality monitor" should be to:

- Evaluate information flow;
- Evaluate FJC and participant roles and their individual confidentiality requirements;
- Evaluate team obligations to maintain confidentiality;
- Ensure confidentiality releases, acknowledgements/agreements are signed;
- Know what resources are available to evaluate confidentiality questions (e.g., Attorney General's office, consultants, or other national experts on confidentiality such as NNEDV);
- Provide for periodic training and evaluation of confidentiality practices; and
- Initiate the (choose one: semiannual/annual) confidentiality audit.

Confidentiality Monitors:
FJC partners are encouraged to understand each partner's confidentiality obligations. The confidentiality monitor can help facilitate training and communication about confidentiality protocols and practices.

Outside Requests for Information

The procedures below are recommendations for protecting confidentiality of victim/client information that is requested from a FJC by non-partners.

Confidential victim/client information should not be provided by a FJC to any non-partner, except that non-identifying demographic information may be provided to evaluators and auditors to evaluate the effectiveness of the FJC. If any victim/client referrals to non-partner service providers are warranted, such referrals should be made in such a way as to preserve confidential victim/client information.

Each partner should have specific protocols for responding to subpoenas, warrants, court orders, and other demands for information that come from outside sources.

Managing confidentiality of victim information in response to outside requests

Subpoenas

Subpoenas are orders to produce information in a civil or criminal case. The subpoena may be directed to the FJC or its personnel or it may be directed to a Family Justice Center victim/client, and may seek discovery of information through testimony or documents at a deposition, or may require the production of testimony or documents at a trial.

Subpoenas directed to FJC victim/clients:
The FJC should not accept service of subpoenas or other documents for any victim/client or person believed to be a victim/client.

Subpoenas directed to the FJC to produce confidential victim/client information, including personal identifying information:

The FJC should not disclose any information without the explicit, informed, written consent of the victim/client. A FJC is under no affirmative obligation to seek a victim/client's release of information or to seek out a former victim/client to advise her of the subpoena. Without full, informed, written consent of the victim/client, the FJC should resist disclosure and make every legal effort to void the subpoena, including filing a Motion to Quash the subpoena, if necessary.

> Subpoenas that seek confidential information should not be responded to by providing the information. To do so could put the victim/client, and the FJC or its partner agency, at risk of liability or harm.

Warrants

Search warrants are orders from a court that give law enforcement officers the authority to search an identified location for specified items or persons. Arrest warrants are orders from a court that give law enforcement officers the authority to arrest specified persons who are suspected to have committed a crime. Arrest warrants generally must be executed at the residence of the suspect, or at another location with the consent of the property owner or manager.

Because of confidentiality, and to encourage victims to have a place where they have access to comprehensive domestic violence services, law enforcement partners at the FJC should agree that

the FJC is not an appropriate place to execute an arrest warrant against a victim/client who is seeking services from the FJC or its partners through the FJC intake process. In addition, law enforcement partners should agree that the confidential information provided to the FJC will not be used as a means of locating and arresting a victim who may be subject to an arrest warrant. If it is discovered that a victim/client who is seeking the help of the FJC is subject to an arrest warrant, the FJC should, with the victim/client's consent, refer her to partners that may assist her with voluntarily surrendering and responding to the arrest warrant.

Court orders

Because of confidentiality, and to encourage victims to have a place where they have access to comprehensive domestic violence services, law enforcement partners for the FJC should agree that the FJC is not an appropriate place to execute a court order against a victim/client who is seeking services from the FJC or its partners through the FJC intake process. In addition, law enforcement partners should agree that the confidential information provided to the FJC will not be used as a means of locating and serving a victim who may be subject to a court order. If it is discovered that a victim/client who is seeking the help of the FJC is subject to a court order, the FJC may, with the victim/client's consent, refer her to partners that may assist her with accepting service and responding to the court order.

Researchers

Confidential victim/client information should not be provided by the FJC to any non-partner, except that non-identifying demographic information may be provided to evaluators and auditors to evaluate the effectiveness of the FJC.

Requests for non-identifying, demographic information should be considered and evaluated by the FJC and should be granted or denied based upon the recommendation of the confidentiality monitor and any specific requirements and limitations that the confidentiality monitor suggests be placed on the use of the non-identifying demographic information.

Public inquiries

Confidential victim/client information should not be provided by the FJC to any non-partner including members of the public, except that non-identifying demographic information may be provided to evaluators and auditors to evaluate the effectiveness of the FJC.

Appendices

A. Confidentiality Checklist
B. Confidentiality “Monitor” duties
C. Confidentiality Audit Check list
D. Client Notice of Rights Form/Confidentiality
E. Victim/Client Limited Release of Information Form
F. SD FJC Client Intake Form
G. SD FJC Confidentiality Agreement
H. SD FJC Confidentiality Agreement Log
I. Authorization to Share Information by Computer
J. Consent Form for Sharing Information at the Family Justice Center

Appendix A

Confidentiality Checklist

Family Justice Centers should implement the following:

- ☐ Confidentiality protocol for the FJC which includes a Code of Conduct
- ☐ Confidentiality protocol for each on-site partner
- ☐ Confidentiality protocol for each off-site partner
- ☐ Notice of rights for clients regarding confidentiality
- ☐ Standard release forms for confidential information
- ☐ A "confidentiality monitor"
- ☐ Quarterly training of at least 60 minutes on confidentiality and privacy issues for victims
- ☐ A plan to do a semi annual or annual confidentiality audit
- ☐ An approved paper or electronic central intake process that collects limited non-identifying information about demographics and services.

Appendix B

Confidentiality "Monitor" Duties

The Family Justice Center and its partners should identify a "confidentiality monitor" whose job it is to review the partnership operation and identify areas where confidentiality can be strengthened. The responsibilities of the "confidentiality monitor" should be to:

1. Evaluate information flow, including technology and electronic systems for maintenance of confidential client information;
2. Evaluate Family Justice Center and participant roles and their individual confidentiality requirements;
3. Ensure confidentiality information is provided to clients, and that releases, acknowledgements/agreements are current, appropriate, and signed when needed;
4. Know what resources are available to figure out confidentiality questions (e.g., Attorney General's office, experts on confidentiality, NNEDV);
5. Provide for periodic training and evaluation of confidentiality practices;
6. Initiate the (choose one: semiannual/annual) confidentiality audit;
7. Analyze requests for information from researchers and others to determine whether and how to respond in a way that is most protective of client information;
8. Hear complaints or concerns from clients about confidentiality issues; and
9. Report to the (Title e.g., Executive Director) on issues related to confidentiality.

Appendix C

Confidentiality Audit Checklist

General Principle: Every step of the audit process and what results should keep safety and justice for domestic violence victims at the forefront of the process, analysis, and decision making involved in the audit. Identify areas where outside support or consultation would be useful to the audit (e.g., contact with a local attorney who is familiar with confidentiality issues related to domestic violence or sexual assault providers, State Coalition resources, an intern or student who could help with the process, etc.).

Also, do the following:

1. Review current laws, rules, regulations, policies, and procedures related to confidentiality;
2. Identify areas within the program that would benefit from a confidentiality audit;
3. Establish a time line for conducting and completing each part of the confidentiality audit

Review current laws, rules, regulations, policies and procedures and practices related to confidentiality

Gather current written policies and procedures related to confidentiality.

1. Review those current written policies and procedures under the guidelines set out below, in order to identify areas where there can be improvement.
2. In addition to identifying and reviewing current written policies and procedures related to confidentiality, identify current practices that implicate confidentiality that are not included in the written policies and procedures, or that are different that what may be contemplated by the current written policies and procedures.
3. If there are no current written policies or procedures of any kind related to confidentiality, identify current practices that implicate confidentiality (e.g., information that may be provided over the phone to callers, responses to requests for information, where and how files are maintained).

Identify areas within the program that would benefit from a confidentiality audit

1. Identify each point of entry that may be used by a program participant to provide confidential information to program staff or volunteers and therefore access services. For example, there may be access through a court restraining order process, through a hotline call, through contact with a first response team, through a *pro se* divorce workshop, through outreach efforts, or by other means. Each point of entry and the process used to get, give and preserve the information of a potential program participant should be evaluated as part of the confidentiality audit.
2. For each point of access, the following questions should be examined:

    a. How is the information provided from the potential service participant to the program staff or volunteer? E.g., in writing, over the phone, in person, by other electronic means?

    b. How is the information provided to the potential service participant from the program staff or volunteer?

c. Where is the information-gathering meeting or conversation held?
d. Who else is present when the meeting or conversation takes place?
e. If the information is provided in writing (e.g., through documents, or by e-mail or fax) what precautions are taken for maintaining confidentiality?
f. What information is requested? (Review intake forms or questionnaires to evaluate what is requested and why).
g. When is anything written down, either by the service participant on a form, or as notes by the program staff or volunteer?
h. Why are these questions asked?
i. Evaluate whether the information is being controlled on a "need to know basis"

Note: For each piece of information requested, there must be an articulated reason for requesting it. The reason must be one of the following only:

1) Essential to meet service participant needs
2) Required by funders or for statistical reporting
3) Necessary to protect the program and its workers from liability

Establish a timeline

1. Set annual or biannual review dates to review confidentiality policies and practices and update them based on legislative changes, policy changes, etc.
2. Identify issues for training and establish a training schedule for staff and volunteers

Appendix D

Client Notice of Rights Form/Confidentiality

As a client of the Family Justice Center, you have the following rights regarding confidentiality of your personal information and communications with Family Justice Center workers:

1. The information that you share with the Family Justice Center will be kept confidential to the greatest extent allowed by law.
2. You may choose what information you want to share with the Family Justice Center. You will not be denied access to services if you choose to not share certain identifying information with the Family Justice Center.
3. The information that you share with the Family Justice Center, including your name, address, phone number, and other personal information will not be shared with other agencies without your permission. Some information about the kind of clients that use the Family Justice Center must be shared with the agency that funds the Family Justice Center, but information that specifically could identify ***you*** as someone who used the Family Justice Center will not be shared unless authorized by you.
4. After your intake with the Family Justice Center, you may choose to be referred to some of our partner agencies for help that is specific to what you need. Those partner agencies include *(Note: List here, names and types of services, if not clear from the description).* You can decide how much, or how little, of the personal information that you have shared today will be shared with each partner agency. You will be told exactly how the information will be shared, and what information will be shared. You will be told, in a general way, what each partner's obligations are to keep your information confidential. If you later decide that you don't want the information that you have shared today to be shared with any of the Family Justice Center partners, let us know and we won't share any more information with those partners.
5. Even though there is confidentiality for the information you share with the Family Justice Center, there are some things that the Family Justice Center workers are required to report even if you don't give permission to report them: suspected child abuse or neglect *(Note: List other things that are reportable, as required by state law, e.g., threats to self or others, elder or at-risk adult abuse, etc.)*
6. If you have any questions or concerns about this notice or your rights, or if you have a concern that your confidential information was not treated appropriately, please contact *(name and number of confidentiality monitor).*

Choose one: Either (1) have client sign that they received, or (2) note in the intake that it was provided to client and reviewed with them.

Appendix E

NNEDV Sample Victim/Client Limited Release of Information Form

FJC LETTERHEAD OR APPROPRIATE AGENCY LETTERHEAD

I understand that _____(FJC or name of agency) has an obligation to keep my information and records confidential. I also understand that I can authorize (FJC or name of agency) to release that information to certain individuals or agencies.

I, _____ (name), authorize _____(FJC or name of agency) to share the following information with _____(specify the name of the person or the specific office of the agency, and address/phone number if known). The information may be shared __ by phone ___ by fax __by mail.

The information that may be shared is:

_____
_____
_____(list as specifically as possible, e.g., name, dates of service, any written documents).

The purpose of such release is:

_____
_____
_____(list as specifically as possible, e.g., representation, to receive benefits).

I have been advised about and understand:

1. The specific information that is to be released;
2. The risks and benefits of releasing the confidential information;
3. That the (*releasing agency name*) and I may not be able to control what happens to the information once it has been released to _____, and that the agency to whom the information is being released may be required by law or practice to share it with others;
4. That a limited release of information can potentially open up access by others to all of my confidential information held by (*FJC or name of ageny)*; and
5. The method by which the information will be released (e.g., phone call, copied documents sent by mail, e-mail, etc.) and the risks of such method of communication.

This release is valid for a period of __15 days; __30 days; _____ 90 days

If additional time is necessary to meet the purpose of this release, I understand that I will need to sign a new release form.

I understand that this release is valid when I sign it, and that I may withdraw my consent to this release at any time either orally or in writing.

_____ **_____**
Signed **Witness**

_____
Date

DATE RELEASE EXPIRES:_____

Appendix F

San Diego FJC Sample Victim/Client Intake Form

SAN DIEGO FAMILY JUSTICE CENTER

Client Intake Form

Date:_____
Intake Specialist:_____
Client Name: First:_____ Middle:_____ Last:_____
Client AKA: First: _____ Middle: _____ Last: _____

Case: _____ Type: _____Case#:_____ Email: _____
Case: _____ Type: _____Case#:_____ Email: _____
Street Address:_____
City/State:_____ Zip Code: _____
Phone#:_____ Email Address: _____

Safe To Call: Y N	Safe To Email: Y N
Safe Place To Contact _____	Safe Phone #: _____
Safe Pager #: _____	Safe Cell Phone#: _____
Safest Day To Call M T W TH F	Safest Time of Day to Call: _____

Birthdate: _____ Marital Status: _____
Gender: M F Pregnant: Y N U
Ethnicity: _____
Children Age: Gender: M F On-Site Today: Y N
Accomp. Victim: _____
Declined Information: Y
Military Affiliation: Y N Military Service Branch: _____
Disability: _____
Phys/Ment Limitation: Y N Priority Special Needs: Y N

Primary Language:_____ Interpreter Needed: Y N
Secondary Language:_____ Sign Language: Y N

Reason for Visiting FJC:_____

Defendant Name: First: _____ Middle: _____ Last: _____
Defendant AKA: First: _____ Middle: _____ Last: _____
Birthdate:

Est. Gross Family Income:_____
How did you find out about the San Diego FJC:_____

Emergency Name: First: _____ Middle: _____ Last: _____
Emergency Phone#:_____

General Comments:_____

I give permission to FJC to enter the above information into a confidential database for statistical purposes.
Signature _____

SAN DIEGO FAMILY JUSTICE CENTER

INTAKE ROUTING SHEET

ROUTING		INITIAL
☐	ADULT PROTECTIVE SERVICES	☐
☐	CENTER FOR COMMUNITY SOLUTIONS	☐
☐	CHAPLAIN'S OFFICE	☐
☐	CHILD PROTECTIVE SERVICES	☐
☐	CHILDREN'S HOSPITAL	☐
☐	CITY ATTORNEY'S OFFICE	☐
☐	DISTRICT ATTORNEY'S OFFICE	☐
☐	EPISCOPAL COMMUNITY SERVICES	☐
☐	FORENSIC MEDICAL UNIT	☐
☐	HOME START	☐
☐	INTAKE COORDINATOR	☐
☐	MILITARY LIAISON	☐
☐	POLICE DEPARTMENT DV UNIT	☐
☐	SAN DIEGO STATE FOUNDATION WIC PROGRAM	☐
☐	SAN DIEGO VOLUNTEER LAWYER PROGRAM	☐
☐	TRAVELER'S AID	☐
☐	UPAC	☐
☐	VICTIM/WITNESS	☐

Appendix G

SAN DIEGO FAMILY JUSTICE CENTER CONFIDENTIALITY AGREEMENT

I, _____, understand that maintaining a client's
(name and position)
confidentiality is paramount to a client's safety.

I am required to keep clients' confidences and may not disclose (including to other project personnel) any information regarding a client without express permission, preferably in writing.

I will not discuss client matters in public spaces, including hallways or open offices and/or conference rooms at the FJC.

I will not publicly acknowledge a client without his/her express permission.

I will direct my questions regarding confidentiality to my immediate supervisor,

_____. If s/he is unavailable, I will direct my
(name and title)
questions to the Director of the Family Justice Center.

I understand that a knowing and voluntary violation of the confidentiality policy can jeopardize my working relationship at the Family Justice Center.

_____ _____
Date Signature of employee

_____ _____
Date Signature of supervisor (if needed)

_____ _____
Date Signature of witness

Appendix H

SAN DIEGO FAMILY JUSTICE CENTER CONFIDENTIALITY AGREEMENT

For the safety and privacy of those using the services at the Family Justice Center, I agree not to disclose to anyone the names, descriptions, or any information regarding any individual I may learn about at the Family Justice center.

DATE	SIGNATURE

Appendix I

Authorization to Share Information by Computer

Thank you for visiting the Family Justice Center today. To make sure you receive the services at the Family Justice Center as quickly as possible, we are requesting your permission to share information by computer to the on-site community partners that you select.

The list of community partners and the services they provide are listed in the attached form and those services will be explained to you by our intake specialist. Only information that you provide on the intake form will be shared with our on-site community partners. We also collect this information to evaluate and improve the overall quality of services available at the Family Justice Center.

All information will of course be completely confidential and only appropriate staff members will see it. Consent is not required to comply with laws regarding mandatory reporting of suspected abuse or neglect or an assessment that there is a danger of serious harm to self or others.

If you agree to share this information by computer, please sign the attached form. If you do not wish to give consent, your services will not be affected in any way.

We are here to help you!

Appendix J

Consent Form for Sharing Information at the Family Justice Center

Please check the appropriate box:

□ I consent to sharing my information by computer to the following community partners:

- □ Camp Hope (off-site summer program for children ages 7 - 12)
- □ Center for Community Solutions (assistance with restraining orders.)
- □ Chaplain's Office (non-denominational spiritual support to victims of domestic violence and their children.)
- □ Children's Hospital (offers programs that provide for the prevention, identification, treatment and rehabilitation of neglected and abused children and women.)
- □ City Attorney's Advocacy Program (informs you of rights and options to assistance and safety planning.)
- □ Home Start (provides therapy and crisis intervention services to victims of domestic violence and children exposed to family violence.)
- □ Forensic Medical Unit (A Nurse Practitioner is available to conduct forensic examinations, to document injuries, and provide limited medical services for victims of domestic violence.)
- □ Military Liaison (assist victims injured by a military member and discuss all of the services available to the victim through the military and civilian communities.)
- □ San Diego Police Department, Domestic Violence Unit (detectives investigate and respond to incidents of domestic violence.)
- □ San Diego State Foundation WIC (Women, Infants and Children) Program (On-site health specialists will provide food assistance and nutrition education for qualified clients and their children.)
- □ San Diego Volunteer Lawyer Program (provides direct representation in court to handle domestic violence restraining order applications, contempt hearings, restitution, and assistance with victims of crime compensation applications.)
- □ Traveler's Aid (help victims get the transportation they need to court appearances, medical and legal appointments, and employment related activities.)
- □ UPAC (Union of Pan Asian Communities) (Translate and assist Asian clients and families with restraining orders, case management, and consultation.)
- □ San Diego Deaf Mental Health Services

□ I do NOT consent to the sharing of my information by computer.

Signature:_____Date:_____