CONFIDENTIALITY AND INFORMATION SHARING CONCERNS FOR ADVOCATES

Loretta Frederick, Battered Women's Justice Project

This outline begins with an introduction to the concept of privileged communications, and the area of data privacy. After explaining the structure and purpose of data privacy laws, the document addresses the legal and ethical issues advocates face as they determine whether and how to share data.

I. Privileged Communications

Privileged communications are those communications recognized as privileged can be protected even from forced disclosure by subpoena.

A. The legal notion of testimonial privilege stems from the English common law, and originates from the determination to protect attorney-client communications from judicial disclosure. When this testimonial privilege exists by law, the communications between a person arid their helper (such as a doctor, lawyer, clergy person, etc) are not discoverable by anyone, and the court cannot force the helper to disclose anywhere, even in court, the information the helper obtained as a result of the communication with the client in the privileged relationship.

B. Generally speaking, the legal system is resistant to classifying any more communications as privileged, because it prevents evidence from being available to the court as it seeks to fairly dispose of the case.

C. There are three sources for privileged communications:

1. Common law, as stated above. Besides the attorney-client privilege, the only other common law privileges granted are for communications between husbands and wives and between jurors.

2. Privileges created by statute.

3. Established through court decision, or case law. There are four factors the court would consider in deciding whether a privilege should be recognized as arising out of a particular relationship, such as battered women's advocate and battered woman.

   a) The communications must originate in confidence that it will not be disclosed.

   b) The element of confidentiality must be essential to the full and satisfactory maintenance of the relationship between parties.

   c) The relationship must be one that, in the opinion of the community, ought to be sedulously fostered.

   d) The injury that would inure to the relationship by the disclosure of the communication must be greater than the benefit thereby gained for the correct

PDF created with FinePrint pdfFactory trial version http://www.pdffactory.com

disposal of the litigation.

D. There are also several different types of privilege: absolute, qualified and semi-qualified. Absolute privilege means with no exceptions the communications arising out of the relationship are privileged. Qualified privilege means limited protection, such as in camera review by a judge who would look at the information to see whether it can be released to the party seeking its release. Semi-qualified privilege allows for specific exceptions in care cases for compelling reasons.

E. It is the client who "owns" the privilege. The client can claim it or waive it. If the client waves the privilege, the agency holding the data must have a different reason to refuse to disclose the information if it wants to refuse to disclose.

F. If a third party is present (including children old enough to know what is going on), the privilege that would otherwise exist is DEFEATED.

II. Data Privacy/Practices Laws and Confidentiality

Data Practices, or data sharing laws, regulate data kept by public agencies or organizations that get funding from certain public entities. The law is very complex and specific.

A. Categories of Data according to MN Data Privacy Laws

1. In Minnesota, data is divided into three categories: public, private and confidential. Public data can be accessed by anyone for any reason. Private data can be accessed by the subject of the data, but not the public. Confidential data cannot be accessed by the subject of the data or the public.

2. Rules related the handling of data may also be categorized by the agency maintaining the data, such as law enforcement or child protective services, and the law may require certain treatment of data depending on these sites where data is kept.
   Example: Data received by the court in an application for an Order for Protection is private data until the papers are served upon the respondent, at which time the data becomes public data.

B. Accessing Data

1. When trying to access data held by governmental entities, and want to be sure of the status of data, contact that person in your jurisdiction (usually a county attorney in the civil division) who is in charge of knowing the data held by the agencies in your jurisdiction.

2. Whenever you are denied access to data, ask the person denying access upon what authority are they denying you access. Often, if people do not know the status of data, they will err on the side of caution and refuse to release it until the question of the legality of its release is answered.

PDF created with FinePrint pdfFactory trial version http://www.pdffactory.com

III. Confidentiality As Required by Funders

A. Where a program receives funding from the Department of Justice, the Department of Health and Human Services, and the Department of Housing and Urban Development, there exist as a condition of funding certain statutory and regulatory restrictions which require it to maintain confidentiality of service participants. Examples include:

1. The Family Violence Prevention and Services Act (hereafter "F VPSA"), 42 USC 10401 *et. seq.,* the Emergency Shelter Grants Program (hereafter "HUD program") 42 USC 11375. *According to* FVPSA, 42 USC 10402(a)(2)(E) (funding applicant must "provide documentation that procedures have been developed, and implemented including copies of the policies and procedure, to assure the confidentiality of records pertaining to any individual provided family violence prevention and treatment services by any program assisted under [FVPSA]").

2. The Victim Compensation and Assistance Program (part of the Victims of Crime Act of 1984)(hereafter "VOCA"), 42 USC 10601 *et. seq*

3. Under VOCA, grantees must certify that they will comply with the regulations set out in 28 CFR Part 22, If the regulations are not adhered to, the program may have sanctions imposed, including the termination of VOCA funding. Any person violating the confidentiality provisions may be fined an amount not to exceed $10,000 plus any other penalty imposed by law. 42 USC 3789g(d). Service participants must be notified that any identifying information will only be used or revealed for statistical or research purposes. 28 CFR 22.27.

4. Domestic violence programs which are granted funds under VOCA are required to follow the regulations in 28 CFR Part 22 which prohibit disclosure of identifying information, require programs to certify that they will do so, and mandate that a program will assure clients that their individual identifying information will not be revealed.

5. The HUD Program laws, 42 USC 1 *1375(c)(5)* say that a grant recipient must certify to the Secretary of HUD that "it will develop and implement procedures to ensure the confidentiality of records pertaining to any individual provided family violence prevention or treatment services

III. Exceptions to Confidentiality Laws

Note: All advocates must disclose to battered women the limits of the confidentiality of the relationship so women can make informed decisions about what to disclose and what to keep secret from the advocate.

A. <u>Multidisciplinary Teams and Collaborations</u>

1. Many states have enacted laws that encourage or mandate the formation of multidisciplinary teams around the issue of child and adult protection or fatality reviews.

PDF created with FinePrint pdfFactory trial version http://www.pdffactory.com

By statute in some states, these teams can share information with each other so long as the data sharing furthers the purpose/mission of the team (generally).

2. Three issues are raised by the rules governing data sharing done by these teams:

   a) Regardless of the statute, the data sharing might not withstand a legal challenge (one could be sued for releasing it or one could be sued to release it);

   b) Regardless of agreements or laws mandating the secrecy of information shared with such group members, information may be released which can harm battered women and their children

   c) This kind of data sharing does not necessarily further the safety interests of battered women and their children in general. For example, where a series of negligent acts by law enforcement may have contributed to the death of a woman, the advocacy program might want to pursue other means (such as wrongful death actions or suits for injunctions) to remedy the wrong. Advocates in possession of protected fatality review information might be constrained from sharing it even where a great injustice has been done and will not be addressed unless it is shared.

3. Issues advocates should consider when participating with Child Protection or criminal justice systems in a collaboration:

   (a) As an advocate on a collaborative team, do you know how the status of the data you share or the data you hold changes once it is shared with any partner to a collaborative? Losing your confidentiality with battered women would strike a blow to your role as a valuable resource for battered women and their children in the community.

   (b) If in the context of the collaboration, do you want to be in a position where you are privy to data that is categorized as "confidential," and which you cannot share with the woman you are advocating for? How does this change the nature of your relationship with her?

   (c) Besides informing the women you work with that you are mandated reporters (usually), you must disclose the extent of their participation on these teams and how this might impact confidentiality, if it would at all.

   (d) People who are working within the criminal justice system, such as for the prosecutor or law enforcement as victim witness advocates do not have confidential relationships with victims and anything told to them must be disclosed to the CJS and where the information is exculpatory (could prove the person is not guilty), the prosecution has the obligation to disclose it to the defense.

PDF created with FinePrint pdfFactory trial version http://www.pdffactory.com

B. Mandatory Child Abuse Reporting Statutes

1. Any confidentiality rules are subject to any child abuse reporting laws. However, mandatory reporting of suspected child abuse and neglect can have the effect of interfering with the trust between the advocate and the client. An advocate, who tells the client that she is "on her side" while at the same time telling her that the advocate must report the client to the authorities if there is any suspicion of child abuse or neglect, can limit the sense of safety the client may have in disclosing to the advocate.

2. Mandatory reports can have serious consequences: child abuse or neglect reports may be made available to courts considering custody or visitation issues. Persons found to have committed child abuse or neglect may be listed on a state registry and prohibited from working with children as child care providers, teachers or even as volunteers in youth programs. A report may put the client at risk of losing her children, or, at the least, of potentially opening up an advocate's records or communications with a client for review by child protective services or other parties in an abuse and neglect or custody proceedings. Advocates subject to mandatory reporting laws should be clear about what constitutes a reportable situation and what activities the advocate must engage in order to fulfill the obligation to report.

C. Duty to Warn

There may be a duty to warn of threats to harm another person, as when a person says they are going to kill another. There may also be a duty to report a person who is in danger of committing suicide or seriously injuring herself Neither of these obligations should cause a program to report in any but the most egregious of circumstances.

III. Issues to Consider When Developing Policy on Handling of Information. For all information that a program is handling, a four-part analysis must be done. This should be a program-wide process that is reviewed annually:

A. What is the purpose for collecting or keeping this particular data? *(Example: the purpose of keeping the name of the battered women in the file is to be able to count her as someone the agency served.)*

B. What would happen if this data got into the hands of the violent partner? *(Example: if the partner found out that the woman had been assisted by the program, he might attack her for planning a separation or for disclosing the abuse to a person outside the family.)*

C. In light of the need for and purpose for keeping it and the risks associated with its release, how we will keep the data? *(Example: perhaps keeping the name of the woman on file for a short time, at least until the reports are completed for funders, would be safe, as long as the information was redacted at a reasonable time in the future.)*

D. If we decide to keep the data, in what form should it be maintained? *(Example: notes from one staff to another about the woman's condition or needs could be put on post-it notes which are destroyed when read.)*

PDF created with FinePrint pdfFactory trial version http://www.pdffactory.com

D. ALL programs must have in place a policy that calls for the regular (such as quarterly) culling of all files in order to ensure that extraneous or dangerous information is not kept.

For more information on confidentiality and information sharing, please contact:

Loretta Frederick, Attorney at Law
Battered Women's Justice Project
2104 Fourth Avenue South, Suite B
Minneapolis, MN 55414
(800) 903-0111, extension 1

PDF created with FinePrint pdfFactory trial version http://www.pdffactory.com