National Domestic Violence Fatality Review Initiative

2014 Vol. II

From the Director

In this issue of our newsletter, the Executive Director of the Confidentiality Institute, Alicia Aiken, J.D., explores confidentiality issues that may arise during the fatality review process. Ms. Aiken provides an overview of the 10 most frequently asked questions regarding confidentiality and suggests resources that may guide teams looking for answers.

We encourage you to access additional resources on our website. It includes an informative webinar video by Alicia Aiken on confidentiality. We would also like to remind you that we will be holding our NDVFRI conference in May in St. Petersburg, Florida. The two-day event will include community panels covering a variety of topics such as risk assessment, data gathering, and the link between fatality reviews and social change, as well as opportunities to participate in mock reviews.

Sincerely,

Neil Websdale, PhD

Program Updates

NDVFRI serves as the national training and technical assistance provider for domestic violence fatality review teams across the country.

In 2014, staff and consultants provided training in eight states:

- Arizona
- Delaware
- Florida
- Indiana
- Montana
- Nevada
- New York
- North Carolina
- Pennsylvania

NDVFRI also hosted a series of webinars on fatality review, an effort that will continue throughout 2015.

- Fatality Review: The State of the Art
- Fatality Review: The Montana Model
- Expanding the Forensic Narrative: Engaging Surviving Family Members in the Fatality Review Process
- Striking a Balance: Confidential Information and Fatality Review

Grant Number: 2009 TA-AX-K076

Confidentiality: Frequently Asked Questions

by Alicia Aiken, J.D.
Confidentiality Institute
Executive Director

The essence of a fatality review is an intensive examination of the past to understand how systems can improve in the future. Of course, access to information about the past is key to the process. However, some information useful to examining the past also lives behind a confidential door, and the deceased victim held the key to opening that door. In those instances, what can the fatality review team do to access the information? And beyond that, what should the team do?

The answer to what the team can and should do to access confidential information will be local and specific to each community. This article maps out a series of questions each team will want to address, along with some resources to find answers. Nothing in this article is intended as specific legal advice, and it is important that teams enlist the assistance of local attorneys to understand the impact of local law on access to information.

When a helping professional is able to reassure a victim that information can be shared and will not be seen by the batterer or the broader community, then it is safer for a victim to open up.

1. Is confidential information ever legally protected after a person's death?

Yes, confidential information often (though not always) remains protected after a person's death. The precise parameters of the protection may be laid out in the statute or regulations that protect confidentiality, may be described in court decisions, or may be imposed by the professional's ethical and licensing requirements.

2. Why would information be protected after the person has died?

For the same reasons information is protected during life – to encourage trust and frank communication within special relationships. Governments and laws protect personal information from disclosure when the broader public benefits from people being willing to communicate. An entire community benefits when open communication leads to effective health care, mental health services, legal advice, and victim advocacy. But some of the information that people share with doctors, lawyers, therapists and advocates is inherently sensitive or embarrassing. At its root, confidentiality during and after life is a promise not to cause harm: share it to get help, and it won't go any further without your permission.

Because people care about controlling their privacy and their reputation after death, public policy routinely supports protecting confidentiality of information after death. The U.S. Supreme Court has recognized the merits of protecting confidential communications after death because "[p]osthumous disclosure of such communications may be as feared as disclosure during the client's lifetime." Swidler & Berlin v. United States, 524 U.S. 399 (1998). A deceased person will have no ability to manage or prevent misuse of information that comes to light after his/her death. The mere possibility that certain information might be disclosed after death can chill a person's willingness to seek help and share freely with helping professionals.

In the domestic violence context, the fear of physical or emotional harm to oneself and loved ones is greatly heightened. Regardless of whether the fear that disclosure will cause harm is well-grounded in fact or a by-product of a batterer's manipulation, that fear has real impact on domestic violence victims' help-seeking behavior. Additionally, concern about public shame or perceived violation of community norms can lead victims to keep secrets about victimization and their own responses to it. When a helping professional is able to reassure a victim that information can be shared and will not be seen by the batterer or the broader community, then it is safer for a victim to open up and actually get the help needed. Therefore, empowering systems to preserve confidentiality actually strengthens the systemic response to domestic violence.

3. How do we determine if and how potentially useful information is legally protected?

The specific protections depend on the particular information at issue and the applicable federal, state and local laws. Some of the most common legal protections

Page 2 -- Continued on page 3

for sensitive information are summarized here. This summary should not take the place of consultation with a local attorney. Every fatality review team should double-check to ensure it is applying the most current version of the relevant law. Where two different laws protect the same information, fatality review teams should generally follow the law that extends the greatest protections over the information.

Medical and mental health information

At the federal level, the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, found at 45 CFR Part 160 and 164, Subparts A and E, protects and controls disclosure of "protected health information". The HIPAA Privacy Rule only applies to "covered entities". The most common covered entity is any health care provider who transmits health information in electronic form for covered transactions. As a broad generalization, HIPAA prohibits disclosure of protected health information without specific consent from the patient or someone with legal authority to act on the patient's behalf. This prohibition on disclosure lasts for 50 years after the patient's death. There are several exceptions to HIPAA's non-disclosure rule, which primarily relate to coordinating patient care, participating in quality control, and responding to emergency situations. For a detailed explanation of the HIPAA Privacy Rule, consult the excellent resource from the Office of Civil Rights, located at www.hhs.gov/ocr/privacy.

In addition to HIPAA, statutory or common law privilege between physicians and patients exists in most, though not all, states. This privilege prevents courts from forcing medical providers to make non-consensual disclosures of information related to a patient's medical care. Doctor-patient privilege can, and often does include exceptions. A state-based privilege may or may not address the existence of privilege after death. However, given the general rule to follow the most protective law, the HIPAA protection should usually prohibit disclosure for 50 years after the patient's death.

Most states also offer some kind of psychotherapist, counselor, and/or social worker privilege to protect information about mental health treatment. Some states have a heightened protection specifically for any mental health information, protecting even the fact that a person sought mental health services. As with other kinds of privilege, the exact definition of protected information, exceptions to privilege, protection after death, and mechanism for releasing information differ depending on the exact statute.

Domestic and sexual violence services information

The Violence Against Women Act ("VAWA") at 42 USC §13925(b)(2) and the Family Violence Prevention and Services Act ("FVPSA") at 42 USC §10406(c)(5) both require that every grantee protect the privacy and confidentiality of victims of violence and their families. The vast majority of domestic and sexual violence service providers in the United States receive some funding through VAWA, FVPSA or both. Some providers may also be covered by HIPAA. VAWA and FVPSA are generally considered to provide stricter rules around information disclosure than HIPAA.

VAWA prohibits all grantees from disclosing personally identifying or individual information collected in connection with providing services, unless there is a written, informed, time-limited release from the person whose information it is. Absent consent, grantees may only disclose personally identifying information if mandated to do so by court or statute. This rule prohibiting disclosure does not apply to court-generated, law enforcement-generated, or prosecution-generated information. And, VAWA does not specify whether this confidentiality survives or is extinguished by a person's death.

The confidentiality language in FVPSA generally mirrors the language in VAWA, including the omission of any language about the effect of death on confidentiality. However, the VAWA provision was updated in 2013 so the two statutes are currently very similar, but not quite identical. The most up-to-date confidentiality language in both VAWA and FVPSA can be found in NNEDV Safety Net's Technology and Confidentiality Toolkit at tools.nnedv.org.

The Victim of Crimes Act ("VOCA") at 42 USC §10601 et. seq. also requires that victim services grantees have policies and procedures to protect the confidentiality of individuals served. One of the express purposes of the regulations implementing VOCA is to "insure the confidentiality of information provided by crime victims to crisis intervention counselors working with victim services programs[.]" 28 CFR §22.1(f). VOCA does not lay out its own specific procedures; rather, it requires that programs lay out their own procedures and follow them, or face an $11,000 fine. 42 USC 3789g(d); 28 CFR 22.29.

Besides federal law, the vast majority of states extend some level of confidentiality and/or privilege to domestic violence and sexual assault victim service providers. A few states also extend protection to communications with human trafficking service providers. The state protections are often stronger than HIPAA, VAWA or FVPSA protections. Disclosure of protected information is even punishable as a crime in some states. The relevant statute may explicitly terminate confidentiality upon death, may specifically continue confidentiality, or may be completely silent on the issue. A Confidentiality Institute summary of specific state protections for victim service providers can be found in SafetyNet's Technology and Confidentiality Toolkit at tools.nnedv.org/tipsheets-charts/charts. The chart is intended to support research and the current law in any state should always be confirmed independently.

A statute's failure to address disclosure after death does not necessarily mean the protection extinguishes at death.

Substance & Alcohol Abuse Services Records

Any federally assisted drug and alcohol abuse provider must also protect the confidentiality of drug and alcohol abuse patient records pursuant to the rules set out in 42 CFR Part 2. The criminal penalty for violating these rules is a monetary fine. The general rule is that no information, including identifying information and any confirmation that a person received services, may be disclosed without the specific, written consent of the patient. Exceptions to this general rule are laid out in the regulations referenced above. If a patient is deceased, a personal representative (as appointed under state law), a spouse or a family member can sign the written consent to disclose records. 42 CFR §2.15(b)(2).

Education Records

As a direct result of the 2013 Campus SaVE Act in the VAWA Reauthorization, colleges and universities are now required to report and respond to domestic violence, dating violence and stalking incidents against their students. Looking into the future, it is very possible that a higher education institution will have information in student records about a deceased person's victimization, a perpetrator's behaviors, and systems' responses to domestic violence. A fatality review team must take note of the Family Educational Rights and Privacy Act and its regulations at 34 CFR Part 99. Personally identifiable information from a student's educational records cannot be disclosed without written consent from the student or a parent if the student is a minor. 34 CFR §99.30. There are exceptions, including an exception for disclosure to "state and local authorities to whom this information is specifically… allowed to be reported or disclosed pursuant to state statute." 34 CFR §99.31(a)(5)(i). Additionally, any recipient of protected educational records must not re-disclose without the consent of the student or parent, and may only use the records for the purposes for which the disclosure was originally made. 34 CFR §99.33(a). As of the publication of this article, the FERPA regulations do not mention the impact of death on access to educational records nor do they provide a specific mechanism for release of records when an adult student is deceased.

Attorney-Client Communications

Every state and federal court offers privilege to the confidential communications between an attorney and a client. The particulars of waivers and the limitations of the privilege are sometimes laid out in local statutes and often modified by court decisions. Under federal law, attorney-client privilege definitely extends after death. Swidler & Berlin v. United States, 524 U.S. 399 (1998). As with other privileges, state statutes may address the issue of death specifically, and they may not.

Religious Official Communications

Similar to attorney-client privilege, every state and federal court offers some protection to communications between an individual and his or her religious official. The breadth of those protections, as well as specific exceptions, will be unique to each state, and is an area of law undergoing much reevaluation and change in recent years, so teams should check the status of the law at least once a year.

4. What if the law in question does not specify what happens after death?

A statute's failure to address disclosure after death does not necessarily mean the protection extinguishes at death. An attorney on behalf of the fatality review team should examine the state's overall approach to confidentiality after death. Are there other statutes, regulations, or case decisions that announce a public

policy of protecting confidential and sensitive information after death? What is the general community understanding of protection of this kind of information after death? What was the reasonable expectation of privacy held by the individual when he or she shared the information?

Fatality review teams should also consider: what will be the broad impact on victim privacy if the team argues that information is not protected after death? Will the same arguments be used to expose victim information to perpetrators? Will living people be endangered by such disclosures? Will the disclosure to fatality review teams inadvertently chill victim willingness to seek help?

5. If the information can only be disclosed with the individual's permission, how can a team ever get access when the person who could sign a release has died?

Every jurisdiction has a procedure for someone else to exercise substitute judgment when a person is deceased or incapacitated. That procedure may differ depending on the type of information being sought. Sometimes, a court order appointing the decision-maker or personal representative may be required. Fatality review teams should become knowledgeable about the local procedures for identifying legal representatives, especially those applicable to the types of information typically sought by the team.

6. Isn't there a disclosure exception for fatality review teams working in the public interest?

There is no automatic confidentiality exception for fatality review teams or other groups working in the public interest. Since confidentiality is typically created by statute, statutes can create exceptions. In some states the law creating the fatality review team explicitly requires certain information to be shared with the team. Ideally, such a law will also set out very clear rules to protect the information once the fatality review team receives it and to prohibit any re-disclosure of information outside of the team.

7. If a fatality review team has an agreement or Memorandum of Understanding requiring confidentiality, can protected information be legally released to the team?

Written agreements that the team will not disclose any identifying information are an important best practice. However, those internal agreements do not change restrictions in federal or state law. Sharing information with a fatality review team counts as a disclosure, even if the team promises that it won't make any identifying re-disclosures. In fact, the internal confidentiality agreement may not be enforceable in a court of law. Ultimately, while an internal confidentiality policy may increase the willingness of community members to voluntarily share with the team, it will not create an exception to the law prohibiting disclosure of protected information.

8. Is there information the team should not access, even if the law says it can?

That is going to be a local, case-by-case decision, but it is a question that should always be asked. Will future victims hesitate to disclose their experience out of fear that their privacy will be invaded after their deaths? If the goals of fatality review are to increase victim access to effective interventions, then any information gathering practices should support and never undermine those goals.

9. If the team does get access to confidential information, what should the team do to keep it safe?

In all procedures and reports, treat the information as valuable, sensitive and private. Establish a clear set of rules about how information is handled, and ensure that every member of the team knows and follows the rules. Review those rules at least once a year. Implement a protocol for information storage and routine information destruction, and then follow it. Encourage every member of the team to be a privacy watchdog and consider assigning one person the role of "confidentiality monitor".

Furthermore, when issuing reports, be careful about the information disclosed about an "anonymous" victim. Ask the question: is it possible to re-identify this murder victim based on the information included in the report? And if so, does the report disclose otherwise private, potentially embarrassing information about that victim (such as mental illness, substance abuse or criminal history)? Remember that murders are typically reported in the media, and the Internet makes local newspapers available to a worldwide audience. Before issuing a report, try running a search based on some of the anonymous individual information included in the report. If it is possible to identify the victims and perpetrators in the report, will the community trust that information is safe with the fatality review team in the future?

Page 5 -- Continued on page 6

10. Where can a fatality review team get specific individualized technical assistance on confidentiality issues?

The National Domestic Violence Fatality Review Initiative can provide technical assistance on a wide array of issues confronting fatality review teams. National Network to End Domestic Violence and Confidentiality Institute specifically provide technical assistance on issues around confidentiality and technology. Teams can request assistance by e-mailing safetynet@nnedv.org and alicia@confidentialityinstitute.org or by making an inquiry at www.confidentialityinstitute.org.

For more information on confidentiality, please visit our website to view Striking a Balance: Confidential Information and Fatality Review, a webinar featuring the author of this piece.
www.ndvfri.org/webinar

Contact NDVFRI

P.O. Box 15026 - Flagstaff - AZ - 86011
Phone: 928.523.3591 -Fax; 928.523-2210
WWW.NDVFRI.ORG
e-mail: NDVFRI@NAU.EDU

Director:
Neil Websdale, Ph.D.
Staff:
Holly Hulen
Adrienne Celaya, Ph.D.
Nathalie Dart
Stephanie Mayer
Nitika Sharma, Ph.D.

This project was supported by Grant No. 2009-TA-AX-K076 awarded by the Office of Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.