SAKI
SEXUAL ASSAULT
KIT INITIATIVE
Reform. Accountability. Justice.

RTI
INTERNATIONAL

Considerations for Sharing Confidential Information across Multidisciplinary Partners

The National Sexual Assault Kit Initiative (SAKI) encourages state and local jurisdictions to form multidisciplinary teams (MDTs) and other multidisciplinary partnerships to make coordinated, community response to sexual assault a fundamental practice. These MDTs are often made of a wide variety of professionals, including law enforcement, forensic medical personnel, forensic laboratory personnel, prosecutors, survivors, community- and systems-based advocates, mental health providers for victims, and research partners. Individuals who participate seek to collaborate to conduct comprehensive case reviews, to understand the nature of sexual assault in the community, and to identify opportunities for improving policies and practices.

To work collaboratively to reach a common goal, individuals within an MDT or similar working group must share information with each other; shared information or data can inform investigations, keep victims informed about the status of their case, or shape community responses by illustrating the prevalence and nature of sexual assault incidents. Determining *what* information to share, *when*, *how*, and *with whom* are consistent questions facing these cross-disciplinary groups.

This SAKI brief highlights important considerations and guidance for the sharing of information among members of MDTs, focusing on key roles that are often involved with SAKI information sharing: law enforcement, crime laboratory personnel, and researchers. This brief considers MDTs as the primary audience, however the content and recommendations can be applied to any professionals who collaborate and share sensitive data across disciplines in this field.

Reasons Collaborators May Share Information

Cross-disciplinary groups share information for a variety of reasons. For example, during case reviews, there can be a need to share information from police reports, laboratory reports, victim and suspect statements, circumstances of the assault, or even personal information about the victim or the suspect to develop a forensic and investigative strategy to move the case forward.[1]

Within their SAKI roles, MDT members may have access to different types of information that, when brought together, help create a more holistic picture of an incident or of the ways that providers could improve their practices to respond to victims. However, individual collaborators likely do not have authorization or authority to access all information to be shared among collaborative members. For example, confidential DNA information may only be available to crime laboratory personnel and law enforcement investigators. However, certain details may be shared by law enforcement with a victim advocate who is interested in keeping the victim apprised of the status of their case.

As another example, MDTs may include or collaborate with researchers to evaluate current practices or to build the field's knowledge base around crime and victimization. In these instances, law enforcement may decide to share aggregate or de-identified information with researchers that excludes sensitive details related to the case, so researchers can analyze trends in crimes and to determine what elements contribute to successful investigations.

[1] National Sexual Assault Kit Initiative. (2018). *A multidisciplinary approach to cold case sexual assault: Guidance for establishing an MDT or a SART* [Brief]. https://www.sakitta.org/toolkit/docs/A-Multidisciplinary-Approach-to-Cold-Case-Sexual-Assault-Guidance-for-Establishing-an-MDT-or-a-SART.pdf .

Types of Information that Collaborators May Share

Accomplishing MDTs' objectives often requires discussion of ongoing investigations, which includes confidential information. Confidential information is any information pertaining to a case that may not be disclosed to third parties unless one is authorized to do so to protect the integrity of an investigation, such as survivor interviews, law enforcement reports, and laboratory results. Sharing confidential information should be limited to those who are actively involved in the case or who have authority to access that information.

Confidential information may include information that is legally protected, such as PII (see text box). PII is protected by the Privacy Act of 1974 (5 U.S.C. 552a, as amended), which outlines fair information practices related to people's personal information.[2] In addition to PII, MDTs often work with PHI (see text box). PHI is federally protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), commonly known as the HIPAA Privacy Rule, which sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. Under these rules the use of PHI *is* permitted without individual authorization for public interest activities (including public health activities, health oversight activities, law enforcement purposes, and research); however, strict security and privacy standards must be followed. Team members with access to PHI are liable for following HIPAA rules.

CJI, often stored in CJI systems,[3] also includes confidential information such as criminal history record, criminal investigative or intelligence information, fingerprints, and investigative or intelligence photographs.[4] When accessing these records, all law enforcement agencies must follow policy and procedures set by the FBI's Criminal Justice Information Services Security Policy,[5] which typically involve training, background checks, and fingerprinting of people allowed to access the information, as well as a strong justification for why individuals need access to these records. Team members who are authorized to access this information may provide such information with collaborators who are also authorized. Public CJI may also be stored in CJI systems and can be shared broadly.

Types of Sensitive Information

- **Confidential Information:** Confidential information is anything that is not available to the general public and contains sensitive information. For criminal justice purposes, it can contain personal identifiable information (PII; as opposed to aggregated data) that is considered private in nature, such as reports of laboratory findings or DNA profiles, law enforcement reports, or survivor interviews.
- **Personal Identifiable Information (PII):** Information that identifies an individual or otherwise provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information about them known. PII is any data that that permits the identity of an individual to be directly or indirectly inferred, including driver's license number, criminal record, and social security number.
- **Protected Health Information (PHI):** Information, including demographic data, that relates to (a) the individual's past, present, or future physical or mental health or condition, (b) the provision of health care to the individual, or (c) the past, present, or future payment for the provision of health care to the individual.
- **Criminal Justice Information (CJI):** Collected by criminal justice agencies, this information is needed for those agencies to carry out its authorized functions, such as the retention of criminal history records and information on incidents, accidents, and wanted persons. It is often stored in criminal justice information systems such as those maintained by state agencies.

Potential Pitfalls When Sharing Information

Although many organizations have established policies related to how and why confidential information can or should be shared, data breaches still occur.

A **data breach** is when confidential or otherwise protected information is accessed by an unauthorized party, or when an authorized party assesses data for an unauthorized purpose.

[2] Office of Privacy and Civil Liberties, U.S. Department of Justice. (2022, October 4). *Privacy Act of 1974*. https://www.justice.gov/opcl/privacy-act-1974

[3] See more at 28 Code of Federal Regulations Part 20: Criminal Justice Information Systems.

[4] Montana Code Annotated 2021, Title 44, Chapter 5, Part 1, Definitions, 44-5-103. (1979 & rev. 2021). https://leg.mt.gov/bills/mca/title_0440/chapter_0050/part_0010/section_0030/0440-0050-0010-0030.html

[5] Criminal Justice Information Services Division, Federal Bureau of Investigation. (2015 & rev. 2019). Criminal Justice Information Services (CJIS) Security Policy (CJISD-ITS-DOC-08140-5.8, Version 5.8). https://www.fbi.gov/file-repository/cjis-security-policy_v5-8_20190601.pdf/view

One common mistake related to information sharing is failing to protect individual identities, thereby making sensitive information accessible to unauthorized parties. This may happen through PII not having adequate redaction or through an individual sharing too much information about a case that allows for the victim or a suspect to be identified (e.g., home address). If certain data can be coded into more general categories or variables that still provide the necessary context, then information specific to an individual case can be removed prior to distribution. For researchers who may have access to names of victims, suspects, or family members, this information should be kept confidential and never be published publicly without the individuals' consent.

Confidential information can also be compromised when it is entered into accessible databases. Team members may use various tools or systems that may or may not protect data against a Freedom of Information Act (FOIA) request, which forces the disclosure of information. Information that contains PII, PHI, or CJI should never be entered into publicly available datasets, such as those a researcher may create to equip others to replicate or expand upon their work. When information is not properly de-identified through coding or redacting privileged information, the privacy and confidentiality of these data are compromised.

In addition to laws that define and protect specific types of information, there are laws and policies that dictate procedures to maintain confidentiality. For example, crime laboratory personnel are charged with adhering to policies that have multiple requirements relating to the limited access, chain of custody, and confidentiality of DNA records and evidence, to guide what information may be shared. These policies provide guidance on who is authorized to access laboratory-related information and for what purposes. Violations of these policies can have serious consequences and result in restrictions on an entire state's ability to use the Combined DNA Index System (CODIS).

Considerations When Sharing Information

All information sharing should be intentional and considered from multiple perspectives, including those of the individual whose information may be shared, the MDT, and the community the MDT serves. Teams should share the level of detail necessary to accomplish a specific goal or task while being fully aware of any confidential information included or data that would enable recipients to establish confidential identifiers. The following questions provide a guide for considering what information to share.

What specifically do we want to know?

Information should be shared for a specific purpose. Thus, before information is compiled, the question(s) to be addressed and purpose must be clear. What is it that the team would like to understand better? The type of question will start to shape the level of information required. For example, understanding general crime trends—such as whether a certain type of crime has increased or decreased in recent years—requires aggregate data only and may be publicly available, whereas understanding gaps in services may require case-level information about individuals' interactions with particular services and where they could have benefitted from intervention.

What information do we need to answer our questions?

If the team determines that case-level information is required, it must be intentional about which specific pieces of information would be helpful. Only information that is relevant to the issue or question at hand should be shared, as opposed to all the information available on that individual case or person. This requires preparation to identify relevant information and/or redact unnecessary information prior to data being shared. As a check on decisions, team members should communicate openly with one another about what information is needed and processes for how they will adapt or redact data to ensure all partners are in alignment with the appropriateness and method of sharing data.

Does everyone need to know?

There may be some sensitive information that a subset of team members can access and analyze among themselves. It may be most appropriate for these members to meet separately to discuss and analyze these data to shed light on a given question because it is unnecessary for identifiable information to be shared with the broader team. Those members may then present the larger findings to the group without compromising data security or confidentiality.

What are the best practices for how data and other sensitive information should be shared and stored?

MDTs communicate in many ways, including in-person meetings, virtual meetings, and email, and this can dictate the medium of information sharing. Regardless of the transmission type, information should be kept secure at all times. Physical copies of information should not be left in the open, for example in a fax machine, but instead should be stored in a locked file drawer when not in use. Information is increasingly shared electronically, but files are vulnerable during digital transfer and are immediately stored in another computer and/or server. It is especially important to ensure that the location of files on the receiving end are secure and only accessible by the intended party. For example, emails containing sensitive information should be encrypted during transfer and downloaded into a secure folder. Email can be avoided altogether by using a secure file transfer protocol, which is accessible only to persons directly involved and protects information both during transfer and storage. Information should be stored only for the limited time in which it is needed, or for the duration required by statute for such information to be retained, and then be destroyed. For example, physical copies can be shredded and digital files can be permanently deleted from devices or removed using file "shredder" software (many kinds are available online for free or at cost). Teams should have an established system for physical and electronic information transfer and storage, and all members should receive training on these practices.

Is everyone on the same page?

It is important to ensure that all members understand when and how to use data for the purposes of the team. Thus, formal protocols are recommended and may take the form of memoranda of understanding (MOUs), data use agreements (DUAs), Institutional Review Board (IRB) approvals, and Certificates of Confidentiality. Such protocols should be considered and established before data sharing begins.

MOUs typically specify shared expectations of the purpose and activities of the team and specific roles. Though MOUs are non-binding, they act as reference guides for the duration of the MDT; even the act of drafting an MOU can help set a clear path for collaboration and the expectations related to information sharing among members. Establishing MDT-wide MOUs on data sharing at the team's start can establish it as a foundational document and provide a common understanding for practices to be followed by the group moving forward.

DUAs dictate what, how, when, and among whom data are to be shared. DUAs are legally binding and required under HIPAA when using certain types of data, such as date of incident or admission, city or zip code, and date of birth or age. Any desired deviation from these documents in practice should prompt discussion to understand why deviation is necessary. If changes are needed to team member roles or expectations or processes related to information sharing, the documents should be formally amended. Discussions and decisions should also be documented to maintain a record of changes.

Practical Application: Sharing of CODIS Hit Information

Policies and standards can limit an MDT's ability to release CODIS hit information to their members, even with the shared understanding that access to this information could increase the chances of case resolution. Therefore, close consideration must be taken to ensure that any steps taken to share CODIS hit information meet all relevant legal guidelines and requirements. Examples of policies and standards include the International Organization for Standardization's (ISO's) Policy 17025, FBI Quality Assurance Standards, the Federal DNA Identification Act, the NDIS Privacy Act Notice and Operational Procedures Manual, and the FBI MOU for use of CODIS.

Bound by the policies and standards described above, many statewide and multijurisdictional SAKI sites have taken measures to safeguard the sharing of CODIS hit information. These measures include implementing laboratory protocol revisions, MOUs, and other types of formal agreements to allow the release of CODIS hit information to criminal justice agencies beyond just the submitting law enforcement agency. When considering this approach, involved parties should always consult with legal representatives. *For examples of these types of agreements related to CODIS hit sharing, please contact sakitta@rti.org*.

Prior to the execution of DUAs or MOUs, a process for amendments should be discussed and included in the agreements. These agreements are sometimes accompanied by non-disclosure agreements, which may serve as a safeguard to protect against the sharing or disclosure of information that may not have been properly redacted or was not intended to be shared.

Individuals conducting research typically seek IRB review and approval (and are required to by federal funders) to ensure that the participants and the data about them are protected. IRBs require researchers to explain their study procedures, how information will be used and collected, and ensure that data are collected with participant consent or in ways that respect the privacy of the data and information accessed. In addition to IRB approvals, researchers may also complete Privacy Certificates or Certificate of Confidentiality. These certificates ensure that information, documents, and other collected information are protected from forced disclosure (e.g., legally compelled to share information). When working with researchers, it may be helpful to request a document that summarizes plans for data collection and protection that are detailed in the IRB and Privacy Certificate materials.

This summary document would describe how the data will be shared, protected, stored, and removed at the end of the study. Such a document could also specify that data should not be emailed to protect the information and how the data will be audited to ensure appropriate access.

Implications and Risks of Data Breaches

When information is not handled or shared securely and appropriately, there are implications and risks for members of the team, individuals involved in the case, the investigations, and the community more broadly.

Both victims and suspects face ramifications if case data or confidential information is released or shared outside of the appropriate avenues. Victims of sexual assault typically share their experiences with select individuals whom they trust. A data breach may publicly identify individuals as victims of sexual assault, taking away victims' autonomy and power to choose whom they disclose their experiences to. In some cases, information about victims that is shared or not adequately redacted violates a victim's right to privacy (for more information about victim's rights in the criminal justice system, visit this resource from the Office for Victims of Crime Training and Technical Assistance Center).[6] The sharing of addresses may put victims at risk for further harm from an offender or suspects at risk from individuals seeking retaliation. Even though suspects may be cleared of suspicion during an investigation, the release of their name as a suspect may impact how these individuals are treated in their community or workplace.

Breaches of information can also compromise investigations. The goals of an investigation are to assess whether there is enough information to build a case against a person who has caused harm and, ultimately, to pass this information along to prosecutors with the goal of keeping the community safe. When investigations are compromised, this can impair public safety because key case information may be excluded from prosecution due to data breaches or concerns about the tampering of information or evidence.

Those who share and receive information may be under regulations and laws that dictate how and what information is shared from their individual institution. When individuals violate these regulations and laws, individuals and the institutions they work for are liable. Of all types of data breaches, inappropriate disclosure of PHI incurs the most severe consequences for those who shared the information. Violation of HIPAA rules can result in civil and criminal penalties. Fines for noncompliance are based on the level of perceived negligence at the time of the violation.

Lastly, data breaches can break community trust in members of the team. Team members each have a responsibility to those they serve to ensure individuals and information about them are treated with respect and care. When data breaches occur, community members may perceive entities who were a part of these breaches to not be trustworthy, which has been shown to be a key consideration for people's willingness to share sensitive information.

Data breaches are a very serious concern and teams sharing information should have a set policy for what happens when a breach is discovered. Recommended elements for such a policy include when and how to notify the individual whose data was breached as well as plans for how to address any other required disclosures.

Conclusion

Information sharing among MDTs and other types of multidisciplinary working groups can be a critical tool for the team to accomplish its goals to address and respond to sexual violence in its community. It is the responsibility of the team and its members to set strong policies and procedures to consider when and how information should be shared. This brief provides recommendations and guidelines for teams to consider when sharing information. Team members should be committed and have capacity to invest significant time and effort not only for formal meetings, but also for establishing strong data-sharing processes to ensure that the team can function effectively while protecting the sensitive information for which they are responsible.

[6] Office for Victims of Crime Training and Technical Assistance Center, U.S. Department of Justice. (n.d.). *About victim rights*. https://www.victimlaw.org/victimlaw/pages/victimsRight.jsp

Authorship

Jaclyn Houston-Kolnik, PhD, Victimization Subject Matter Expert, RTI International. Dr. Houston-Kolnik provides training and technical assistance (TTA) on trauma-informed and victim-centered practices and programming to support victims' help-seeking and healing, with a specific focus on collaborative and multidisciplinary approaches to gender-based violence.

Stefany Ramos, PhD, Community and Interpersonal Violence Prevention Expert, RTI International. Dr. Ramos conducts research on systemic strategies for prevention of non-accidental injuries, including improving collaboration between multidisciplinary organizations at various levels, data monitoring, and evaluation.

Ashley Rodriguez, Advanced DNA Testing Subject Matter Expert, RTI International. Ms. Rodriguez provides insight into advanced DNA forensics testing strategies and leads the creation of TTA materials associated with advanced testing strategies (including forensic genetic genealogy) in support of investigating cold case sexual assaults, sexually motivated homicides, and cold case violent crimes.

With contributions from:

Dr. Kevin J. Strom, PhD, Director, Center for Public Safety and Resilience, RTI International. Dr. Strom directs the Center for Public Safety and Resilience at RTI International, which conducts research, technical assistance, and training across topics related to policing, investigations, and violence prevention. He leads the SAKI TTA project, which supports state and local jurisdictions from across the country in testing, investigating, and prosecuting cases associated with previously unsubmitted sexual assault kits. He also leads the National Case Closed Project, a nationwide effort designed to support law enforcement agencies in improving their violent crime clearance rates, with an emphasis on fatal and nonfatal shooting cases.

Jennifer D. Naugle, Deputy Division Administrator, Wisconsin Division of Forensic Sciences. Ms. Naugle has been at the Wisconsin State Crime Laboratories (under the state's Department of Justice) since 2009 and has been the Deputy Division Administrator since 2019. Jennifer has worked in the field of forensics for almost 20 years in positions ranging from practitioner through executive management. Ms. Naugle has also worked on various initiatives in the field of forensics and currently serves on national committees for forensic science policy and national advocacy. She is an affiliate of the Organization of Scientific Area Committees for Forensic Science, a member of the Midwestern Association of Forensic Scientists, a technical assessor for ANAB, a founding member of the National Association of Forensic Science Boards, a member of the National Technology Validation and Implementation Collaborative, and the current Past-President of the American Society of Crime Laboratory Directors.

Matthew Gamette, Laboratory System Director, Idaho State Police Forensic Services. Mr. Gamette serves as the Chair of the Consortium of Forensic Science Organizations, as well as an affiliate Organization of Scientific Area Committees member on the Forensic Science Standards Board's Terminology Task Group and chairs its subcommittee for terms development. He was selected by the U.S. Department of Justice to participate as a member (ongoing) on the Forensic Laboratory Needs – Technology Working Group. He also serves on the federal Centers for Disease Control and Prevention (CDC)–National Institute of Justice Working Group on Data Exchange in Medicolegal Death Investigation. Mr. Gamette served as an elected board member of the American Society of Crime Lab Directors for over 7 years, as president from 2018–2019. He currently assists with its Accreditation Initiative. He founded and chairs the National Technology Validation and Implementation Collaborative Steering Group. He has been a peer reviewer for the SAKI grant program and Capacity Enhancement for Backlog Reduction competitive grant program at the Bureau of Justice Assistance.

Dr. Rachel Lovell, PhD, Director of the Criminology Research Center, Cleveland State University. Dr. Lovell is an Assistant Professor of Criminology and Director of the Criminology Research Center at Cleveland State University in Cleveland, OH. She is an applied criminologist and methodologist whose research focuses on gender-based violence and victimization, particularly sexual assault, human trafficking, and intimate partner violence. She is an established scholar with over $6.7 million in external funding for research since 2013, numerous peer-reviewed publications and chapters, and the lead editor on a recently published monograph, *Sexual Assault Kits and Reforming the Response to Rape* (Routledge Press).

This project was supported by Grant No. 2019-MU-BX-K011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the U.S. Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice. **For more information, visit www.sakitta.org.**

SAKI 15254 0623