


RTI INTERNATIONAL

Center for Court Innovation

An Evaluation and Sustainability Resource Brief

Ensuring the Confidentiality of Participant Data in Reentry Program Operations and Evaluation

Why Confidentiality of Study Participant Information Is Important

Reentry programs collect and store sensitive, *personally identifiable information* about the clients they serve as part of typical program operations. This information (PII) may include client background characteristics and needs, referrals provided, services received, and outcomes achieved. The information collected can often be extremely useful for other providers working with the client or for the agency's external research partner. PII on program participants may be necessary for other reasons, such as enabling a grant-funded program to report performance metrics required by its funding source. For example, Department of Justice (DOJ) Second Chance Act grantees may be required to report recidivism performance metrics for program participants; they must collect personal identifiers to do so.[1]

Despite the value of collecting myriad data points from and about reentry program participants, and the many ways this information could be beneficial, program staff and research partners do not have the right to use client information however they would like. Program staff and clients have a relationship of trust, and some of the client information collected by program staff is extremely sensitive and private. Therefore, an expectation exists that the information collected will not be disclosed to others without the

Key Definition

Personally identifiable information (PII): Information that can be used to distinguish or trace an individual's identity. Examples of PII include

- name;
- personal identification numbers, such as Social Security Number, passport number, driver's license number, correctional identifier, taxpayer identification number, or financial account numbers;
- address information, including street address;
- personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); and
- information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

[1] For example, arrest, conviction, and incarceration metrics are required to be reported for individuals participating in Second Chance Act programs funded by the Bureau of Justice Assistance. This reporting requires maintaining personal identifiers for program participants so that their recidivism outcomes can be searched from databases maintained by criminal justice agencies.

Ensuring the Confidentiality of Participant Data in Reentry Program Operations and Evaluation

Key Definition

Release of information (ROI): A document that allows the participant to decide what information they want to release from their file, whom they want it released to, how long that information can be released, and under what statutes and guidelines it is released.

client's permission, as specified in a consent form or *release of information* signed before program enrollment. Similarly, if a program evaluator or research partner collects data from program participants, participants should be able to trust that this information will be kept confidential and securely protected, and they should be aware of situations in which this information would have to be disclosed.

A breach of confidentiality occurs when information about a client is disclosed to a third party without the client's consent or when clients suffer the consequences of careless privacy practices. Often, a breach of confidentiality is the result of the actions, or failure to act, of one or more individual employees. As one example, sensitive client information could be obtained by a third party through a data breach. Importantly, a breach of confidentiality by even an individual employee can result in many adverse impacts to the entire business entity. A breach of confidentiality may result in the following consequences to the parties involved:

- Lawsuits and payment of monetary and punitive damages
- Loss of business clients, partners, and other relationships
- Termination of employment
- Filing of criminal charges

Key Definition

Human subjects research: Research involving a living individual in which an investigator

- obtains information through intervention or interaction with the individual and uses, studies, or analyzes the information or biospecimens or
- obtains, uses, studies, analyzes, or generates identifiable private information.

Examples of human subjects research include a person who willingly participates in research or individuals who are not actively participating in research but whose data are obtained from medical records, surveys, observation, or third parties for the purposes of research.

This brief discusses best practices in protecting and ensuring the confidentiality of participant data. Your agency should establish procedures for the access, transmission, storage, and disposal of information in accordance with basic ethical standards governing research activities. We provide tips that are relevant to reentry practitioners seeking to protect client data as well as to research partners who are collecting or working with data as part of their evaluation.

This brief is not intended to convey regulatory guidance; additional regulations specific to your agency/organization, funding source, or other governing body may apply. In particular, human subjects requirements governing research activities that are classified as *human subjects research* may apply, and research staff should consult with their organization's institutional review board (IRB), compliance officer, or research committee to determine whether this classification applies and, if so, to identify and comply with the requirements. For example, DOJ-funded projects classified as human subjects research must be

reviewed and approved by an IRB (28 CFR Part 46).[2] Reentry program staff and research partners should also identify and comply with other regulatory requirements specific to the program's funding source to ensure confidentiality of data. For example, in addition to the IRB requirement, DOJ-funded projects must protect identifiable information on private persons involved in research (28 CFR Part 22).[3] Grantees who conduct a research project that will collect PII must submit and maintain a current privacy certificate to DOJ, specifying that PII will be used only for the purpose for which the information was obtained and outlining the procedures in place to ensure the confidentiality of identifiable data. Finally, *covered entities* and those working with *protected health information* (PHI) are subject to requirements under the Privacy Rule of the Health Insurance Portability and Accessibility Act of 1996 (HIPAA) and should make sure they are familiar with these rules and requirements.

Ensuring the confidentiality of client data in your reentry program evaluation involves establishing and following procedures for the access, transmission, storage, and disposal of PII and PHI in accordance with your agency's or organization's policy, the terms of your contract, and applicable laws or regulations that pertain to your work with human subjects.

Key Definitions

Covered entities: Individuals, organizations, and agencies that must comply with HIPAA's privacy and security rule requirements and must provide individuals with certain rights with respect to their health information.

Protected health information (PHI): All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral, that is protected information under the Privacy Rule of the Health Insurance Portability and Accessibility Act of 1996 (HIPAA). Examples of PHI are

- treatment or medical records,
- mental health diagnoses, and
- same data elements as PII if information originates from a covered entity or its business associate.

Informed consent: The process by which human subjects are informed about the research activity and decide whether to participate

Guidelines for Maintaining Data Confidentiality

This section presents guidelines for maintaining data confidentiality, beginning with the type of data you acquire and how you manage access to those data files and keep them secure. These guidelines assume that you have already collected the data you will be maintaining and that when you obtained *informed consent* from your program participants, you informed them of what data you would be collecting, how you would store the files, and in what specific manner the data would be used.

[2] https://ecfr.io/Title-28/Part-46

[3] https://www.ojp.gov/funding/explore/legaloverview2021/researchrelatedrequirements

Ensuring the Confidentiality of Participant Data in Reentry Program Operations and Evaluation

Helpful Tips to Consider for Ensuring Confidentiality During Primary Data Collection

The tips in this brief pertain to protecting data once collected, but researchers and program staff should also follow best practices in ensuring confidentiality during data collection.

- If collecting participant data using a web-based survey platform, **use a secure survey platform** that protects survey data, transmits encrypted information, uses IP whitelisting, uses a secure connection, keeps records of IP addresses for tracking respondents, and protects against spamming. (For a summary of web-based survey platforms and their security features, see https://nationalreentryresourcecenter.org/resources/fact-sheet-comparing-web-based-survey-platforms).
- If collecting participant data through focus groups, **establish confidentiality procedures** such as having the participants agree to keep one another's input confidential (but alerting participants to the fact that the researchers cannot control what other participants divulge and that this should be kept in mind during the discussion), having participants use an alias instead of their name, and not including any PII in the focus group notes.
- For all data collection activities, **inform participants of mandatory exceptions to confidentiality** (if applicable, depending on state laws) when getting their consent for data collection activities. For example, some states consider researchers to be mandatory reporters for child abuse or neglect, and some correctional institutions require researchers to disclose threats of harm or planned escapes.

- **Understand the type of sensitive information you are storing.** First, take the time to understand what personal information you have in your internal case management or data collection systems and on your computers. Is this information classified as PII or PHI (see the Key Definitions sidebar)? This distinction could affect the security environment in which the information should be (or is required to be) stored. Relatedly, it is important to assess the risk level of this information. As a best practice, entities that store sensitive data on individuals in their internal information systems typically conduct risk and threat assessments to determine the likelihood and impact of a breach of confidentiality and then use the results to implement data security practices.[4]
- **Limit the amount of PII/PHI you are gathering.** Consciously determine the amount of data that is actually necessary for your programmatic operations and research purposes. Reducing confidentiality risk can be accomplished by minimizing the amount of sensitive information obtained or stored. If data can be collected anonymously in the first place (e.g., a client satisfaction survey that does not need to be linked to other data sets), that is preferable to collecting identifiable data. If identifiers are needed—which is often the case when data from various sources need to be linked together using a common identifier (e.g., name, correctional identifier)—remove the identifiers as soon as the files are linked. Also, consider using a study identification number that is not PII to identify individuals in the linked data set (with a crosswalk between the two identifiers maintained separately and kept secure).
- **Encrypt sensitive files.** A best practice when protecting sensitive data is to ensure that the data are unreadable to anyone except those who have the appropriate credentials and are authorized to view the data. Encryption can be applied to storage devices (data "at rest") and to network data (data "in flight"),

[4] https://itsecurity.uiowa.edu/resources/everyone/determining-risk-levels; https://files.nc.gov/ncdit/documents/Statewide_Policies/Statewide-Data-Class-Handling.pdf

with the latter discussed in the next section. The type of computing device, network communicating from and to, and extent to which PII or PHI is involved will dictate whether or not encryption should be used. Encryption is not needed if you do not store or work with research data that include PII or PHI. For more information on encryption tools and other recommendations related to encryption, visit https://www.security.uci.edu/secure-computer/encryption.html

- **Manage data access.** Regardless of how sensitive your participants' data are, ensure that only authorized individuals have access to data you are storing. Data access by authorized individuals should be periodically reviewed and revoked when it is no longer necessary.
- **Physically secure devices and paper documents.** Protect digital devices and paper documents that contain client data by storing them in a locked area. Never leave sensitive documents or devices in public locations.
- **Securely dispose of data, devices, and paper records.** Appropriately dispose of data when they are no longer necessary. This means securely erasing the data so that they cannot be recovered. Electronic files (including backup files) should be destroyed or erased, and physical documents should be shredded.
- **Manage data utilization.** Use sensitive data only in ways that have been approved by your human subjects committee or IRB (if applicable) or conveyed to clients when they provided consent. Using participants' data for a purpose outside of standard program operations or the planned research study would be a violation of participants' trust.
- **Manage devices.** Adopt essential security practices with devices on which data are stored, including computers, tablets, or other devices. These practices might include using anti-virus software, using a whitelisting application, using device passcodes, suspending inactivity, enabling firewalls, and using whole-disk encryption. Relatedly, client data files should be saved on a network (with enhanced security features) as opposed to someone's personal computer or external hard drive that has not been approved for storing that information.
- **Train team members on best practices in managing confidential data.** Program and evaluation team members who work with confidential data should understand and follow data security practices outlined in this section. Additionally, it is best practice to have authorized staff sign a confidentiality agreement in which they agree to comply with data access and storage protocols.

Data confidentiality guidelines are intended to avoid the worst-case scenario that might result from a breach of confidentiality with regard to sensitive data, such as data files being intercepted, hacked, or viewed by people who are not allowed to view the information.

Even though the likelihood of a breach of confidentiality may seem very low, the *consequences* of such a breach for the people whose data are breached might be quite severe. This is particularly the case with a justice system-involved population, such as individuals under supervision, subject to court-ordered conditions, and so on. These individuals might be at risk of criminal justice sanctions, loss of employment, or other adverse consequences if their sensitive information were to be seen by others.

- **Develop an incident response plan.** In preparation for the possibility that a participant's confidential information is breached (either accidentally or intentionally), organizations should devise an incident response plan to quickly respond to data breaches. By responding quickly, an entity can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result. The plan will need to outline what information will be reported to leadership or other appropriate personnel and when. Importantly, the plan needs to describe when and how the breach will be communicated to clients. The plan should also outline how staff will record how they became aware of the data breach and the actions taken in response. Keeping records on actual and suspected breaches will help you proactively manage future events and identify risks that could make a breach more likely. Specific information in an incident response plan includes how to define and identify a data breach, whom to report a data breach to, and how the plan will apply to various types of data breaches, as well as processes for responding to incidents that involve another entity, strategies for assessing risk and impact levels of data, and regular review and testing of the response plan.

Guidelines for Transmitting Sensitive Information

Often in reentry program operations or evaluation, client data collected by one entity are shared with another entity for service provision or research purposes. Data sharing can minimize client burden, create data collection efficiencies, and leverage data as much as possible. However, to keep the client's data secure, follow several guidelines when transmitting client data from one agency to another.

- **Ensure you have permission to share or receive data.** As a critical first step, a determination must be made about whether permissions are needed from clients to ensure that the data can be shared through a release of information. Also, a data use agreement (DUA), data transfer agreement (DTA), or memorandum of understanding (MOU) may need to be executed between one agency and another, or between an agency and a research partner, to allow data sharing. If the provider of data is a covered entity (CE), a *business associate* agreement (BAA) may need to be executed between parties before information is shared.

Key Definition

Business associates (BA): Individuals, organizations, businesses, and vendors that assist a covered entity with implementing its health care activities and functions and that are required to execute a written business associate contract or agreement with the covered entity. This business associate agreement (BAA) must establish the specific roles and activities of the BA and how the BA will comply with the same privacy and security rule requirements that covered entities must follow to protect client health information.

- **Never email sensitive information in the body of an email message.** The use of email on its own without encryption (discussed below) is a nonsecure method for transmitting sensitive information. When an email is transmitted, it travels across a series of networks and servers to reach the recipient, often in human-readable text. During that time, it is possible for hackers to intercept it without detection. Even at rest, the information is at risk of being intercepted. A copy of each email message is typically stored on the sender's and recipient's computers, servers, and possibly a backup server (physical or in the cloud). Relatedly, some agencies may have policies prohibiting the transmission of sensitive information to and from personal email accounts.
- **Encrypt emails and password-protect attached files.** Some study protocols allow for PII, PHI, or proprietary and sensitive information to be transmitted via email. However, it is critical to protect the data against a breach. Therefore, encrypting emails and, if attaching files, password-protecting the files may be necessary. Common email platforms often support these features. For example, Microsoft Outlook has an encryption option, and most file types allow the file to be password-protected. Passwords should be strong, meaning that they include a combination of numbers, letters, and symbols. Importantly, after transmitting the message/files, disclose passwords or encryption keys (to enable the recipient to open the email or file) only through a separate process, such as a separate email or a telephone call.
- **Use a secure file transfer program.** If you are receiving or transferring files that contain PII, PHI, or other proprietary and sensitive information, a secure file program such as Secure File Transfer Protocol (sFTP) is recommended over other methods such as email. An sFTP site is an electronic file tool that allows entities to access sensitive information provided by another entity. Documents stored on the sFTP server are not automatically encrypted, so a two-step file encryption and transmission process will be needed. In the first step, the sender changes the settings of the file, so that recipients must enter a password (which the sender will relay separately) to open it. In the second step, the sender transmits the encrypted file to the recipient by uploading it to the sFTP site for the recipient to access. Both the sender and recipient will need credentials to access the sFTP site (e.g., host, username, password).
- **Encrypt sensitive information stored on external storage devices.** In some instances, sensitive data may need to be physically mailed to an external partner. To protect against a breach should the mailing be intercepted, the sensitive information stored on CDs, DVDs, hard drives, USB flash drives, floppy disks, or other removable media should be encrypted before the media are mailed or shared.

Ensuring the Confidentiality of Participant Data in Reentry Program Operations and Evaluation

Summary

Maintaining the confidentiality of participants involved in your reentry program operations or evaluation is an important obligation for program and research staff. Reentry program participants are a particularly vulnerable population, not only from a human subjects perspective (given the limited rights and potential for coercion for those under criminal justice system supervision), but also given the high level of need and barriers facing them as they transition from a correctional institution into the community. Program participants need to develop trusting relationships with service providers and freely share information about themselves that will assist these providers in helping them and tracking their progress. Keeping their private information confidential is the ethical thing to do. In addition, following confidentiality procedures is also important from a liability perspective, given the many adverse legal and personal consequences (to clients, program staff, and researchers) associated with a breach of confidentiality, even if unintentional. Following the guidelines provided in this brief will help reentry programs and research partners protect their clients' data, minimizing the risk of a breach and the negative consequences of any breach that might occur.

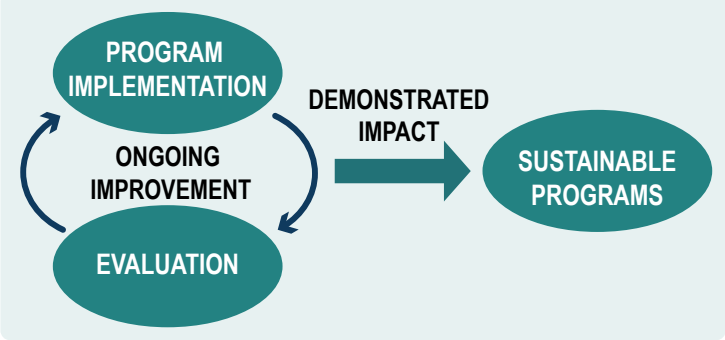
Resources

https://www.unr.edu/research-integrity/human-research/human-research-protection-policy-manual/410-maintaining-data-confidentiality

https://research.uci.edu/human-research-protections/research-subjects/privacy-and-confidentiality/

The Evaluation and Sustainability Training and Technical Assistance Project

The Evaluation and Sustainability Training and Technical Assistance (ES TTA) Project supports Second Chance Act (SCA) grantees in conducting more rigorous evaluations that lead to data-driven program improvement and demonstrated impact and that support programs' long-term sustainability. For more information about the project, contact ESTTA@rti.org.



The ES TTA Project is conducted by RTI International and the Center for Court Innovation with funding from Grant No. 2019-MU-BX-K041 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the 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.

RTI INTERNATIONAL

Center for Court Innovation

Suggested citation: Scaggs, S. J. W., & Lindquist, C. (2022). Ensuring the Confidentiality of Participant Data in Reentry Program Operations and Evaluation. U.S. Department of Justice, Bureau of Justice Assistance.