Brief Overview of Data Privacy & Security Considerations at Harm Reduction Programs

Developed by,

Sarah Deutsch, MPH

With the Supporting Harm Reduction Programs (SHaRP) team,

Sara Glick, PhD, MPH
Elise Healy, MPH
Kelly Knudtson, MPH
Lesly-Marie Buer, PhD, MPH

SHaRP: SUPPORTING HARM REDUCTION PROGRAMS
UNIVERSITY of WASHINGTON
School of Medicine

Contents

Statement of Purpose 2
Why is data privacy and security important at harm reduction programs? 2
What are the differences between confidential and anonymous services? 3
What is HIPAA and does it apply to my program? 3
What is a Covered Entity and how do we know if our program is one? 4
What is protected health information (PHI)? 4
What is a Business Associate Agreement (BAA)? 5
What privacy and security measures should we take, regardless of our HIPAA determination? 5
What special privacy and security considerations should online or mail-based programs take? 7
What is linkage to care and how can we do it safely? 7
What considerations should we make when reporting out data? 8
What other resources are available to me? 8

Statement of Purpose

This brief FAQ document aims to provide an overview of some important data privacy and security considerations for syringe services programs (SSPs) and harm reduction programs. As harm reduction programs grow and modernize, it is important for them to formalize data privacy and security practices so that they can be responsible stewards of participant data, whether digitally or on paper. However, because harm reduction programs often straddle the health care and social services fields, and many are grassroots organizations with less formalized infrastructure, the practices and procedures they should have in place when it comes to data privacy and security may not always be straightforward.

While the following document contains some recommendations for good practices and measures programs might take to ensure participant data privacy and security, it does not provide in-depth or detailed instructions and is not intended as implementation guidance.

Notably, this document was developed by a team that is well-versed in general data hygiene practices, but our team members are not educated in legal matters. Any information that might appear to support programs in understanding and adhering to laws related to data privacy and security should be vetted first by legal counsel.

Why is data privacy and security important at harm reduction programs?

Data privacy and security is critical for any business or service operation to establish and maintain trust with their constituents, and to minimize potential risks and threats. Harm reduction programs interact with and serve criminalized populations and often straddle the grey area between social services provider and health care provider, further complicating their data safety needs. Privacy and security should be the cornerstones of harm reduction program planning and development, including transparency about data privacy and security practices to establish trust with participants.

Risks to data privacy and security are primarily related to the possibility of data being accessed and subsequently traced back to the identity of the individual. Risks may be related to the potential for unauthorized access, or to actual unauthorized access. Examples include:

- Staff member A accidentally emails unencrypted data to staff member B, who does not have authorization to access these data. The potential for unauthorized access exists as soon as the email is sent; it becomes actual only if staff member B downloads the data. Unauthorized access could also occur if the email was intercepted by a cyberattack.
- Staff member C is granted access to confidential participant data when their job responsibilities do not include direct contact with participants. While the data access is authorized, it increases risk to participant privacy.
- A third-party vendor receives a legal subpoena that compels them to share Organization A's dataset with law enforcement. While this is an example of authorized access to data, it poses a risk to participant privacy.
- Staff member D identifies that paper files and a laptop with participant data stored on it were stolen out of the outreach van over the weekend. This is an example of potential unauthorized access.

Organizations are responsible for stewarding and safeguarding their participants' data and minimizing data collection to ensure the smallest risk possible if a breach occurs. It is also important for Harm reduction programs, particularly those that provide a combination of anonymous and confidential services, to be aware of whether HIPAA applies to them, and work towards compliance.

What are the differences between confidential and anonymous services?

Anonymous services are services that are not accompanied by documentation of individual level data that could be potentially identifying. In these cases, even the service providers would not be able to trace any documentation back to a specific encounter with a specific individual.

For example, Program A provides anonymous services because they document only service-level data, like how many syringes and doses of naloxone were distributed to a given participant and limited individual-level data that is not demographic, health-related, or otherwise indirectly identifiable.

By "otherwise indirectly identifiable data," we mean data that may be contextually traceable. For example, if Program B collected participant housing status and no demographic data or health-related data, but only one participant reported living in their car, this data could become potentially traceable. While providers may be confident that anonymous data is not identifiable, they should not guarantee privacy or security to their participants, since there is usually a chance that someone overheard the encounter, or that a breach may occur in the future.

Confidential services are services that are accompanied by documentation of any individual level data that could potentially be identifiable when combined with other information. For that reason, confidential data poses a greater risk to a participant than anonymous data. Any harm reduction program that enrolls participants using an intake form, or assigns a unique ID by another means, is likely providing confidential services. Even without a unique ID, if a harm reduction program collects demographic data and/or health-related data, they are likely conducting confidential services. When conducting confidential services, providers should never guarantee privacy and security, because even with the best practices, no programs are exempt from risk.

Even if a harm reduction program provides anonymous access to syringes, it is extremely common for the program to offer some confidential services, as well – for example, case management, HIV testing, or HCV (hepatitis C virus) testing. In these cases, it is important for the anonymous data to be stored separately from, and not linked to, the confidential data – otherwise, they would no longer be anonymous.

In general, as programs consider whether they can feasibly offer anonymous services to their participants, they should still strive to collect the least amount of data possible to reduce risk and increase willingness to participate.

What is HIPAA and does it apply to my program?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] is a federal law that mandates U.S. Health and Human Services (HHS) to create national standards to prevent health information from being disclosed without an individual's consent or knowledge, while allowing health information to be shared when necessary to facilitate collaboration across the healthcare system.

The **HIPAA Privacy Rule** is the implementation side of the law. The rule describes how entities subject to the law (covered entities) can use and disclose an individual's health information. It also includes standards for individuals' rights to control how their health information is used. Essentially, a covered entity is not permitted to use or disclose protected health information, except when: a) explicitly authorized by the Privacy Rule, b) to the individual who is the subject of the information, and c) to those

[1] https://www.cdc.gov/phlp/publications/topic/hipaa.html

who the individual has specifically authorized in writing. All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.

A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. Additional guidance on Minimum Necessary is available at the HHS website.

What is a Covered Entity and how do we know if our program is one?

A covered entity (CE) is any organization subject to the Privacy Rule. There are three primary types of covered entities. Most importantly, all healthcare providers that electronically transmit health information, such as referral authorization requests, benefit eligibility inquiries, claims, or emails containing e-PHI, are covered entities. Additionally, health plans that pay for the cost of medical care are also covered entities, as are healthcare clearinghouses that process health data.

The HIPAA Privacy Rule[2] requires covered entities to 1) notify individuals about their privacy rights and how their information can be used, 2) adopt and implement privacy procedures, 3) train their employees to understand the procedures and designate an individual to be responsible for implementation, and 4) secure records containing identifiable health information.

If you are unsure whether your SSP meets the criteria for a covered entity, you can complete the decision tree here.[3] There are also experts who can help you review your services and activities to identify whether you are a covered entity or a business associate.

What is protected health information (PHI)?

All health information (such as demographic data, medical history, test results, insurance information, etc.) that contains at least one individual identifier is considered protected health information (PHI) under the HIPAA Privacy Rule. This information can be in any form, whether electronic, paper, or oral. The Privacy Rule names 18 individual identifiers that, when combined with health information as described above, become PHI. Common identifiers that harm reduction programs may use include names, any component of an address, all elements of dates related to an individual *except* years of birth, phone numbers, and email addresses. However, any other characteristic that could uniquely identify the individual should also be considered an individual identifier. The below example illustrates how unintuitive the differences can be:

- Race (considered health data) saved with the month of birth (considered an individual identifier) would be considered PHI.
- HIV testing history (considered health data) saved with the year of birth (not considered an individual identifier) would **not** be considered PHI.

The **HIPAA Security Rule** is specific to protecting individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form, also called e-PHI. CEs are responsible

[2] https://www.hhs.gov/hipaa/for-professionals/faq/189/what-does-the-hipaa-privacy-rule-require-the-average-provider-to-do/index.html

[3] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf.

for ensuring the confidentiality of all e-PHI, detecting and safeguarding against anticipated threats to the security of the information, protecting against anticipated impermissible uses or disclosures, and certifying compliance by their workforce.

What is a Business Associate Agreement (BAA)?

A Business Associate Agreement[4] is an agreement between a HIPAA Covered Entity (CE) and another entity that provides services to the CE. This entity is the Business Associate (BA). The BAA specifies certain standards and safeguards that will ensure HIPAA compliance. The agreement outlines what practices are expected of the BA in order to protect the CE's data, and what procedures to follow should any violation or data breach occur. A common example of a business associate are third-party IT support and software vendors that store CE data. Two or more CEs can also be business associates of each other – for example, if you work with another organization to provide HIV testing onsite, then you may be business associates. Any harm reduction programs that are not CEs may be business associates of CEs – for example, if they provide hepatitis C medical case management for a clinic – if they may come into contact with PHI that belongs to the CE.

Because a CE may not authorize its business associate to make any use or disclosure of PHI that would violate the HIPAA Privacy Rule, business associates are obligated to adhere to similar procedures as they would if they were a covered entity themselves. Additional information and a sample agreement can be found here.[5]

When writing or reviewing BAAs, pay special attention to if there is an indemnification clause, which lays out if there is any fiscal responsibility for handling the resolution if a privacy breach occurs.

What privacy and security measures should we take, regardless of our HIPAA determination?

While most of the below recommendations are encompassed by the HIPAA Privacy Rule that covered entities must implement, not all harm reduction programs are subject to the full extent of HIPAA requirements. Therefore, as opposed to adhering to a law that does not apply to them, these organizations should instead aim to develop and institute privacy and security practices that are likely to result in protection for their participants.

Overarching recommendations for harm reduction programs include:

- Ensure that at least one team member has developing and maintaining privacy and security policies and procedures as a dedicated component of their scope of work and weekly workload.
- Train team members in privacy and security practices. Because privacy and security measures are only effective if they are consistently implemented, once harm reduction programs set policies, it is important to train team members and perform regular monitoring to make sure they are familiar with and following the policy. Remember, even if 9 of your 10 team members follow protocol, your data would be considered compromised!
- All harm reduction programs should conduct a data inventory, meaning cataloging all the data that they collect and the systems they use to collect and store it. Seeing a list of all data you collect in one place will help you assess your risks. This can be accomplished by creating a table

[4] https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
[5] https://www.hhs.gov/sites/default/files/model-business-associate-agreement.pdf

that includes information on what data you collect and what level of sensitivity each data point carries, and how each data point is collected, where it is stored, who has access to it, and what it is used for. This may also include if, when, and how a program deletes or destroys past data that is no longer needed.

There are several privacy measures harm reduction programs should take. They include, but are not limited to:

- Minimize the amount of data collected. Ensuring only necessary data is stored by the program limits the overall risks that could occur in the event of a breach, and that the overall impact is as small as possible.
- Minimize linked data to the extent possible (e.g. unique IDs, linking point in time data to service data, linking SSP service data to other non-medical services)
- Take steps to ensure data collection activities are conducted where they are least likely to be overheard.
- Execute memoranda of understanding (MOUs) with all partners who share space and might overhear any encounters, or mistakenly take a piece of paper that has participant data on it.
- Limit access and use of participant data to team members who need it to carry out their job functions.
- If a program uses software that has log ins,
    - Ensure each team member has their own log-in and they are not shared. This is both for security reasons, because human error is one of the most common ways that unauthorized access to data occurs; and for privacy, because participants have a right to limit who sees their data to essential people.
    - Train team members to log out when not using the platform so that it cannot be accessed by another person
- Communicate your privacy practices to your participants, and any risks they might be taking by participating in your program.

Similarly, there are several security measures harm reduction programs should take. They include, but are not limited to:

- If any participant data is stored on devices, these devices should be encrypted. Additionally, devices that are taken off site should have a “checkout” system. All devices that store participant data should be stored securely when not in use, ideally with physical locks.
- Conceal the identities of participants when communicating about them with other team members and avoid SMS and email unless the data is encrypted.
- Use multi-factor authentication and automatic logouts for all logins, including computers, email inboxes, and data management software.
- Turn on automatic updates for all devices and applications.
- Train team members to recognize phishing attempts and install anti-malware and anti-virus software on organization devices.
- Carefully review the business and data practices of all third parties who might come into contact with your data, ideally with legal support, to ensure they are taking appropriate steps to safeguard it. This includes IT consultants, printer and fax companies, software you might use to enter/analyze/store your data, cloud computing companies, etc.
- Communicate your security practices to your participants, and any risks they might be taking by participating in your program.

- Communicate any data breaches to your participants, and what steps you are taking to mitigate the breach.

Note that each of the above will look different in practice at every program, and there is no one-size-fits-all approach to privacy and security. For example, perhaps at one program, staff notify participants of their privacy practice verbally, while at another they are distributed to every participant. What is most important is that every program has a standard practice that is implemented consistently.

What special privacy and security considerations should online or mail-based programs take?

Because online and mail-based programs utilize digital systems to communicate with their participants; and often need to collect contact information such as full names, email addresses, and mailing addresses; they face significantly greater inherent privacy and security risks. In addition to the recommendations above, there are a few critical steps an online or mail-based harm reduction program can take to improve privacy and security for their participants. These include, but are not limited to:

- Masking the IP addresses of anyone submitting an order.
- Collecting contact information separately from any other participant data, such as supply requests (orders). Ideally, contact information would be stored on a separate platform from any health information to further limit risk.
- Purging mailing addresses data periodically. You can still keep ZIP code data to map programmatic reach.

What is linkage to care and how can we do it safely?

Linkage to care is defined in many different ways, often by funders, and generally involves obtaining confirmation from participants or their providers about their engagement in care. Harm reduction programs often face challenges with this both because of the fluid nature of their participants' lives, and the necessity to protect confidentiality at the expense of typical health care documentation practices. Usually, this requires documentation of more detailed health information and contact information of participants. And, because data is being transmitted, it is likely that programs that offer linkage to care services are subject to HIPAA.

Regardless of a harm reduction organization's HIPAA designation, there are some additional privacy and security considerations harm reduction programs might take:

- Develop a consent form that informs participants about what agreeing to this follow-up entails (i.e., who you will be contacting, using what methods, and what data might be disclosed).
- Ensure participants sign a release of information (ROI) for every provider you might be in communication with. ROIs should specify what data might be disclosed, how it will be transmitted, and include an expiration date, after which time you will no longer be able to contact this provider. You will likely want to utilize the ROIs provided by the specific provider. If you use your own form, the provider may refuse to release the information to you! You can usually find an ROI on the provider's website or request it by phone.
- Engage providers who you often share participants with to educate them about your services and establish an ongoing relationship to improve care for your participants. Consider executing MOUs to articulate your organizations' relationship. The difference between an MOU and a BAA is that an MOU deals with the relationship between the entities other than expectations around data management. Sometimes, two organizations might have both an MOU and a BAA in place.

What considerations should we make when reporting out data?

When analyzing data, it is important to keep a few general security considerations in mind. First, any analyses that are displayed digitally should be detached from the source data. This is especially important for data dashboards. Since some dashboard software accesses data stored on another platform, hackers may be able to gain access to the source data using the same pathway. As a result, harm reduction programs should work with a software company that offers end to end encryption. Generally, harm reduction organizations would only want to use data dashboards for internal use. If applicable, individual level identifiers and unique IDs should be removed from the dataset, and when sharing any analyses from the dashboard, they should just be snapshots rather than a live link.

Additionally, because harm reduction programs often provide services to a relatively small population, data that is stratified may result in analyses where only a few participants have a given characteristic. In this case, even in anonymous datasets, there may be risk of identification (i.e., in a table that shows age by race, and there is only one person in the 70+, Indigenous cell, would it be feasible that a viewer could identify that person?). As such, programs should consider suppressing data for categories that have small numbers. Challenges around equity and accurately capturing disparities may arise, so we recommend consulting with an epidemiologist at your local or state health department if you have further questions about suppression of small numbers.

What other resources are available to me?

While privacy and security can be overwhelming, there is information available online, and some experts may also offer live support as you work to strengthen your practices. A few of these resources are listed below, although this list is not comprehensive.

Network for Public Health Law, Harm Reduction Legal Project[6] offers legal expertise to harm reduction organizations and may be able to offer insight into privacy and security topics.

NEXT Distro,[7] an online provider of harm reduction supplies, has resources to support mail-based programs.

The U.S. Department of Health and Human Services[8] has an extensive guide to understanding HIPAA. Although it can be challenging to dig through so many resources, there are extensive FAQs that can support your organization as it explores this topic area.

Surveillance Self Defense[9] has a number of resources, including how-tos, for safer online communication and a module on creating a security plan.[10]

hacking//hustling,[11] a sex-worker led organization, offers consultations and trainings about digital security.

---

[6] https://www.networkforphl.org/resources/topics/projects/harm-reduction-legal-project/

[7] https://nextdistro.org/faq

[8] https://www.hhs.gov/hipaa/index.html

[9] https://ssd.eff.org/

[10] https://ssd.eff.org/module/your-security-plan

[11] https://hackinghustling.org/consulting-services/