Table of Contents

1. Introduction

Protection of client confidentiality is a major concern for persons living with HIV/AIDS (PLWHA), who may face discrimination, harassment, or victimization should their diagnosis become known. Fear of unauthorized or inadvertent disclosure often prevents individuals living with HIV from accessing HIV-related information and services. Agencies funded under the U.S. Department of Housing and Urban Development's (HUD) Housing Opportunities for Persons With AIDS (HOPWA) program must develop and carefully implement confidentiality procedures to protect the identity of individuals who inquire about and/or receive HOPWA services.

1.1 User Guide Overview and Objectives

This user guide provides information on maintaining confidentiality for HOPWA providers of all types – including grantees, project sponsors, subcontractors, and subrecipients – in all the roles they may serve – including program administrators, managers, front-line staff, and monitors. The purpose of this guide is to help HOPWA providers sort through the questions that arise when protecting confidential client information.

This user guide presents various "best practices" outlining suggested steps that HOPWA providers can take to protect client information. Not all of these best practices will apply to each agency and not all of these best practices may be feasible for all agencies. Additional resources, listed at the end of this section and referenced throughout this user guide, may also be helpful in HOPWA administration and program management. A checklist is included as an Appendix and provides a quick reference for implementing confidentiality practices.

The privacy of confidential client information must be considered during all phases of grant administration and service delivery including collecting, storing, and sharing client data, as well as during a monitoring visit. Each HOPWA provider has unique circumstances that will guide decisions regarding the type of information collected from clients; how it is stored, used, and reported; how it is shared during monitoring visits; and how to respond if a breach of confidentiality occurs. This publication serves as a general guide for thinking through the issues related to protecting the confidentiality of client data in order to develop or enhance agency policies and practices.

User Guide Objectives

- Provide broad context of confidentiality laws and regulations
- Support the development and/or review of policies and procedures designed to protect client information
- Review ways to maintain confidentiality when data is collected, stored, shared, and reported
- Provide guidance on conducting monitoring visits in a manner that protects confidentiality
- Discuss methods to address data breaches

This user guide is organized in the following manner. First, it provides information on HOPWA-specific requirements as well as a general overview of laws and regulations that may be relevant to HOPWA providers. Second, it discusses the role of written policies, procedures, and training. Third, it reviews aspects of program operations that are key to protecting confidentiality. Fourth, it discusses elements for HOPWA providers to consider regarding the monitoring process. Finally, it provides recommendations for addressing data breaches.

1.2 Confidential Information

Protecting client privacy requires an understanding of what client information is considered confidential. This document focuses on the confidentiality requirements and expectations of the HOPWA program, which may differ from other federal, state, and local confidentiality requirements. HOPWA regulations state that the names of individuals must remain confidential. Other personally identifying information includes any data that, alone or in conjunction with other data, is likely to disclose a client's identity and/or location. In small or largely homogenous communities, identification of personal client characteristics such as race/ethnicity, gender, age, or address can lead to the disclosure of an individual's HIV status. It is important, therefore, to not limit protection to an individual's name, but rather to protect any and all information that could lead to the disclosure of an individual's identity and their participation in HIV services or programs.

1.3 Additional Resources

HOPWA Grantee Oversight Resource Guide
See Chapter 2: Developing an Oversight Plan
See Chapter 3: Basic Oversight Elements
https://www.onecpd.info/resource/1003/hopwa-grantee-oversight-resource-guide/

Data Security and Confidentiality Guidelines
Center for Disease Control National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention
http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf

CPD Monitoring Handbook
See Chapter 10 on HOPWA Monitoring
http://www.hud.gov/offices/cpd/library/monitoring/handbook.cfm

2. Laws and Regulations

This section references the HOPWA regulations related to confidentiality as well as other laws and regulations. The intent of this section is to provide an understanding of HOPWA confidentiality requirements and offer a broad overview of other confidentiality laws that may apply to HOPWA providers. HOPWA providers may wish to speak with an attorney to determine which privacy laws and regulations apply to their specific programs.

2.1 HOPWA-Specific Requirements

The AIDS Housing Opportunity Act of 1992,[1] the law authorizing the HOPWA program, requires that grantees and project sponsors protect the privacy of those receiving HOPWA assistance (See Section 856 of the Act). The HOPWA regulation, 24 CFR 574, implements this requirement and states:

> *The grantee shall agree, and shall ensure that each project sponsor agrees, to ensure the confidentiality of the name of any individual assisted under this part and any other information regarding individuals receiving assistance (24 CFR 574.440).* [2]

This broad regulatory language, intended to ensure confidentiality for HOPWA clients, has many implications. To provide further guidance, HUD addressed HOPWA program expectations for client confidentiality in Section II(a) of HUD's Community Planning and Development (CPD) Notice 06-07, which states:

> *HIV/AIDS status, along with related client eligibility documentation, should only be accessible by qualified individuals who determine eligibility or provide support,*

[1] The AIDS Housing Opportunity Act of 1992 is available online here: https://www.onecpd.info/resource/2934/aids-housing-opportunity-act/.
[2] The HOPWA regulation 24 CFR 574.440 is available online here: http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=64b4e621c18fef131cebcd977b7de916&rgn=div8&view=text&node=24:3.1.1.3.7.5.1.5&idno=24.

or who oversee the provision of this federal assistance. Grantees must have written procedures and training efforts in place to maintain confidentiality. Precautions may include, but are not limited to, maintaining paper files in locked cabinets accessible only by designated individuals, and installing security software for electronic files. Grantees should conduct periodic monitoring of these procedures and undertake related training efforts (CPD Notice 06-07).[3]

Grantees must ensure both that their own organization protects client confidentiality and that their project sponsors agree to ensure client confidentiality, according to 24 CFR 574.440. In order to confirm that project sponsors are aware of this mandate, HOPWA grantees should include provisions within each project sponsor agreement or contract outlining the confidentiality requirements for any recipient of HOPWA funds. If a HOPWA project sponsor contracts with a subrecipient or subcontractor to perform HOPWA funded activities, the project sponsor should also pass along these requirements as appropriate. All organizations receiving HOPWA funds should have a clear understanding of their role and responsibilities in following HOPWA program rules related to confidentiality. Failure to comply is considered a default of grant responsibilities and could result in HUD monitoring findings, suspension, loss of grant funds, or other potentially negative consequence including legal action.

Key HOPWA Regulatory and CPD Notice Provisions

- Ensure the confidentiality of the names and other identifying information of individuals who receive assistance
- Ensure that adequate protections are in place to protect confidentiality
- Maintain written policies and procedures on confidentiality
- Train staff on confidentiality issues
- Conduct periodic monitoring of confidentiality procedures

2.2 Other Laws and Regulations

HOPWA providers often administer or manage multiple programs with various funding streams. Providers must be aware of general and HIV-specific confidentiality requirements imposed by each funding stream as well as federal and state laws that protect HIV-related or other health-related information. These laws and regulations may be relevant to HOPWA providers in carrying out HOPWA funded activities in coordination with services funded by other sources.

[3] The CPD Notice 06-07 is available online here: https://www.onecpd.info/resource/2781/notice-cpd-06-07-standards-hopwa-strmu-payments-permanent-housing/.

A wide range of federal laws include provisions related to privacy. The following list is not exhaustive but is provided to indicate the scope of federal privacy laws.

Examples of Federal Laws with Confidentiality Provisions

- Americans with Disabilities Act
- Confidentiality of Alcohol and Drug Abuse Patient Records
- Electronic Communications Privacy Act
- Heath Insurance Portability and Accountability Act
- Violence Against Women Act
- Victims of Crime Act
- Affordable Care Act

Most states and some local jurisdictions have laws that specifically protect HIV-related information or outline requirements regarding HIV-status disclosure.[4] These statutes include a variety of provisions that must be considered. HOPWA providers must follow all applicable federal, state, and local laws and regulations, in addition to meeting the HOPWA requirements.

Health Insurance Portability and Accountability Act (HIPAA)

The overall goal of the HIPAA is to make it easier for medical providers to share and transfer information in order to provide quality care. If an organization is covered by the HIPAA, client consent is needed to share health information.

The HIPAA Privacy Rule applies when **all** of the following criteria are met:

- The agency is a health care provider.
- The agency conducts certain covered transactions, such as billing an insurance provider.
- The agency conducts these transactions electronically.

Housing-only providers are not necessarily covered by HIPAA; the entity must also provide health care. Additional guidance is available from the Centers for Medicaid and Medicare online here: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/CoveredEntitycharts.pdf.

[4] Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization: http://epic.org/privacy/medical/cdc_survey.html.

3. Policies, Procedures, and Training

As discussed earlier, HOPWA grantees are mandated by HUD's CPD Notice 06-07 to have "written procedures…[and]…training efforts in place to maintain client confidentiality." Grantees must be able to document that these requirements are met. In addition, grantees should review existing legal agreements with their project sponsors to determine if they have effectively passed these standards to their project sponsors. All HOPWA providers should maintain written policies and procedures and train staff to ensure compliance.

3.1 Policies and Procedures

Developing or reviewing policies and procedures is a good starting point from which to consider how to protect client confidentiality. Agency-wide confidentiality policies and standard operating procedures should be consistent with other agency policies and procedures. These policies and procedures are fundamental in creating and maintaining agency practices that ensure a client's private information will remain confidential.

Agency decisions about collecting and using personal information should be done with respect for the individual and in the context of federal, state, and local laws and regulations. Client information is sensitive and personal. There should be a business purpose behind what information is collected and how it is handled. Internal agency disclosure of confidential client information should be on a need-to-know basis only.

A confidentiality policy is a written statement that illustrates an agency's guiding principles for how it will use and treat client information. The policy should also reflect an agency's values, goals and standards while outlining a broad course of action. A standard operating procedure (SOP) is a written guide that provides instructions on how the confidentiality policy will be implemented or operationalized. The process of developing a SOP can help an agency think through the necessary steps in collecting, storing, and using client information.

Questions to Consider when Developing Policies and Procedures

- What personal information of clients is subject to HOPWA or other privacy protections?
- When does confidential information need to be shared?
- How will consent for data sharing be obtained and documented?
- Who will participate in the process of developing or reviewing policies and procedures?
- How will the agency ensure policies and procedures are understood and upheld?
- How often and under what circumstances will policies and procedures be reviewed and updated?
- How and when might confidential information be shared unintentionally?
- How will data breaches be handled?

Information to Include in Policies and Procedures

- A statement about the importance of protecting client data
- The name and title for the confidentiality and data management point of contact for the agency
- The process for gathering, recording, and storing confidential information
- The process to obtain consent to release confidential information when necessary
- The standards for how data inquiries, data sharing, and reporting will be handled
- A statement that the agency will adhere to due process when handling client complaints about privacy issues
- A protocol for dealing with a breach in confidentiality
- The method and frequency of training staff members on policies and practices surrounding confidentiality
- The forms to be utilized for client consents and interagency data sharing

An additional strategy for developing policies and procedures is to review activities that occur during program operations. Each operational activity should be fully considered to ensure that confidential information is protected during the entire service delivery continuum from intake to service provision to reporting. Table 1 outlines questions and best practices for each activity.

Table 1: Developing Policies and Procedures

Activity	Questions	Best Practices
Gathering Data	What information is collected? Why is it collected? When is it collected? How is it obtained from the client?	Only collect data that is pertinent to determining eligibility, serving the client, and essential for reporting and evaluation in a manner that protects confidentiality.
Storing Data	How and where is the data maintained and stored? What information is protected by law or regulation?	Protect information stored electronically and on paper according to applicable laws and regulations and in a manner that limits access appropriately.
Sharing Data	With whom is confidential information shared? What consent must be obtained? What purpose does the data sharing serve? How is the information shared?	Only share information if /when necessary and in the best interest of the client, with the proper client consent and in a manner that protects confidentiality.
Reporting	What data is required to report to funders? How is the information shared?	Fulfill all reporting requirements in a manner that protects confidentiality.
Monitoring	What is monitored? Where and how often does monitoring occur? Who performs the monitoring?	Fulfill all monitoring requirements in a manner that protects confidentiality.
Addressing Data Breaches	How did the data breach occur? Has breached data since been secured? Have necessary parties been notified? What steps will prevent a future breach?	Respond to data breaches in a manner that resolves immediate confidentiality threats and takes action to prevent future occurrences.

3.2 Confidentiality Training

Grantees must establish a method to ensure all grantee and project sponsor staff is trained sufficiently in protecting client confidentiality. All staff – including management, front-line, and administrative – should be fully informed and regularly trained about confidentiality policies and procedures. New staff should be trained upon beginning their job.

Confidentiality Training Topics

- Importance of protecting confidentiality
- Identifying what information is protected and why
- Obtaining and utilizing valid consent forms
- Protecting both hard copy and electronic data usage and storage
- Avoiding unintentional data sharing
- Responding to breaches of confidentiality

Training can be provided in many ways. Hosting formal sessions dedicated solely to confidentiality issues, providing written notices or reminders, conducting or participating in online training, and incorporating confidentiality discussions within regularly scheduled staff meetings may all contribute to an agency's overall capacity. HOPWA providers should consider the nature of the training method, staffing patterns, and agency activities in determining when and how often staff receive training. Training efforts should provide sufficient opportunities to keep all staff updated on current policies and new developments, identify and clarify items that may be complex or misunderstood, and obtain feedback on procedures that may need improvement. Staff confidentiality agreements acknowledge and document that staff members have received training on, understand, and agree to the established confidentiality policies.

4. Program Operations

When reviewing client confidentiality protections during each stage of program operations, it is helpful to consider the following activities: 1) gathering client data for purposes of eligibility determination, service delivery, research, and evaluation; 2) maintaining and storing client data for documentation purposes; 3) sharing client data to coordinate services with other providers; and 4) reporting client data for program compliance, research, or evaluation. Concerns related to monitoring, an additional key operational function, are discussed later in more detail.

4.1 Gathering Client Data

HOPWA providers need to collect an array of data on each household served with HOPWA funds. Data collection is an integral part of ensuring that programs serve eligible households

with appropriate eligible services in accordance with the regulations. The data is also important for performance reports, research, and evaluations.

Collect Client Data through Private Intake Sessions

Typically, when a client first goes to an agency to receive services, staff members conduct an initial intake and assessment. During this activity, staff members document the client's demographic, family and medical information, service history, and needs. The intake session is often the first opportunity to give and receive information from a potential client. A successful intake session is critical to building trust.

Best Practices for Collecting Client Data

- Conduct the intake session in a private room, where the client and staff person can talk without the risk of other staff or clients overhearing
- Explain, in detail, the agency's information sharing policies
- Communicate to the client who in the agency is responsible for handling questions or complaints about confidentiality
- Ensure that the client understands the agency's information sharing policies and procedures
- Provide appropriate time for the client to review and sign forms
- Provide a written copy of client rights (including confidentiality) and signed consent form
- Provide interpretation and/or documents translated into the appropriate language when necessary
- Post confidentiality notices in the intake room and around the agency

Discuss Privacy Policies and Obtain Consent Forms during Intake

Consent forms, also commonly referred to as releases of information, are essential to requesting and documenting permission to share a client's confidential information. Ideally, consent forms would be discussed and obtained during the first interaction, typically the intake session. However, when necessary, allow extra time for a client to understand and discuss consent with others. Consent forms can be obtained at any point prior to releasing or sharing protected information.

A consent form documents that the client grants the agency permission to share protected personal information with an identified entity for a specific and stated purpose and time frame. A general or blanket consent form, therefore, is not appropriate. The intent of sharing information should be thoroughly explained to all clients and clearly stated on the form.

The period of time during which consent is permitted may depend on its particular purpose or may be defined by the client. A consent form must be fully executed with the client signature (or legal guardian, if applicable) and date. Typically, the effective time of consent forms should be no longer than one year, after which time a new consent should be obtained. A client may revoke or withdraw their consent at any time after signing.

Best Practices for Consent Forms

- Identify what information the client agrees to share
- Explain why and with whom the information will be shared
- State how the client may revoke or cancel their consent
- Define the time period during which consent is granted
- Obtain the client's signature (or legal guardian, if applicable) and date

4.2 Storing Client Data

Once client data gets collected, it must be safely stored and protected to minimize the risk of an information breach. There are several precautions involving staffing, physical space, and computer security that an agency should consider when storing client information.

Staff Precautions: Limit the Number of Staff with Access to Client Data

An agency should consider which staff positions have a relevant need to know protected client information and only those staff should be granted access to such information. This consideration extends to staff members who perform record-keeping, data collection and/or data management tasks. Limiting the number of staff members who handle data also facilitates consistent data entry leading to improved data quality.

Hard Copy Precautions: Keep Written Records Safe and Secure

All written documentation of confidential information must be safeguarded to prevent it from being seen by unauthorized individuals. Various storage methods can be implemented to protect hard copy client files. HOPWA providers need to consider their particular agency's needs, resources, and environment in order to develop precautions that will effectively ensure written document security. HOPWA providers that must also meet other non-HOPWA confidentiality requirements (e.g. 42 CFR 2 and/or HIPAA) must consider how to meet these distinct standards for all clients.

Best Practices for Protecting Written Records

- Institute a unique client identification coding protocol
- Use a unique client code, rather than client names or personal identifiers, to label files
- Label exterior of files "confidential" in a clear and noticeable way
- Label contents of files "confidential" in a clear and noticeable way

- Store client files in a secure location and in a cabinet that remains locked
    - Locate the file cabinet in a locked room
    - Lock the cabinet after each use
    - Designate which staff members need access to client files
    - Do not leave the keys in the cabinet
- Limit access to and track location of files
    - Use a tracking sheet with unique clients codes to sign in/out files from cabinet
    - Identify with whom and where the file will be located
    - Access files only when needed and return files to the cabinet when not in use
- Do not leave files unattended on a desktop, in an office, or other unsecure areas
- Use envelope style or accordion-like files, binders, and/or fasteners to protect against paper inadvertently falling out of files
- Develop a system to securely identify and store closed files
- Develop protocols if transporting confidential information off site
    - File protected information in a separate file that does not leave the office
    - Redact names and other identifying information
    - Only transport files out of the office in a locked and secure container
    - Only transport files out of the office when absolutely necessary
- Develop protocols for confidential information disposal
    - Shred all confidential paper documents prior to disposal
    - Consider contracting with a professional disposal service that follows appropriate confidentiality practices

Electronic Copy Precautions: Protect and Limit Access to Electronic Data

The same rigorous standards discussed above regarding written records apply to confidential client information in electronic form. HOPWA providers need to pay particular attention to evolving technologies for maintaining electronic records. As with paper files, considerations regarding particular environments and resources affect how to develop effective precautions to safeguard electronic client data.

Best Practices for Protecting Electronic Data

- Designate computers, servers, and/or server regions that store or provide access to client data
- Password protect all computers and servers that store and/or provide access to client data
- Locate the server in a secure area
- Limit the number of staff authorized to access the server that stores client data

- Assign a unique log-on or user ID and password to each authorized staff member
    - Note that unique user identifiers are useful in tracking information for auditing purposes and data breach investigations
- Password protect unique electronic client records
- Require passwords to be re-entered when a computer has been idle for a defined time period
- Authenticate users for internet-based systems by implementing a user ID and password system
- Terminate access to all confidential electronic records when staff members leave the agency or no longer perform a job function that requires access to client data
- Overwrite or degauss (erase) all electronic data

4.3 Sharing Client Data

An agency that provides comprehensive and coordinated services to clients often needs to share client data with other organizations. Each agency should carefully consider what information is needed, when information is needed, and how information will be shared.

Ensure Client Consent Is Obtained

As discussed, HOPWA providers must protect the identity of all clients and, therefore, must obtain consent forms prior to sharing any protected information. Before sharing such information, verify that a valid consent form is on file.

If an agency regularly shares information with another specific entity, consider obtaining that consent at intake. For example, a HOPWA project sponsor providing tenant based rental assistance may have a formal agreement with and a standard practice to refer clients to an external supportive service provider. In this instance, a consent form for that specific supportive service provider and purpose could be obtained at intake.

Discuss How to Protect Shared Client Information

HOPWA providers should discuss their need, if any, to share confidential client information with another agency. An agency should first conduct an internal review of their needs regarding what, when, and how to share this information. After that review is complete, the agency should then approach external entities. These discussions should be informed by agency policies and procedures for handling client information and should focus on how to provide appropriate and timely referrals and services. At all times, information should be shared only on a need-to-know basis and only when client consent has been obtained.

An agency that regularly shares confidential information with another agency may find it useful to establish a formal agreement outlining information sharing practices, such as what, how, and

when information will be shared. This agreement is typically referred to as a Participation Agreement (PA) or a Memorandum of Understanding (MOU). Specific confidentiality requirements and privacy practices may vary across agencies depending on the type of funding received and the population served. The practices of each participating agency should be fully understood by all parties to an agreement.

Considering the Need for a Participation Agreement

- How often and how much information needs to be shared?
    - Note that while all data must be protected, the frequency and amount of information sharing may influence how the process is designed.
- How will the information be shared and stored?
- What protocols are needed to ensure information reaches only the intended recipient?
- Do protocols for all agencies address how information is shared (e.g., fax or email)?
- What protocols are needed to ensure that confidential information will be protected and not shared again with another third party without consent?

Best Practices for Developing a Participation Agreement

- Ensure that there is a shared understanding of confidentiality policies and practices amongst all participating agencies
- Be aware that agencies that do not traditionally or primarily serve clients with HIV/AIDS may be less familiar with the particular requirements for protecting a client's HIV status
- Be familiar with the each agency's consent form
- Identify and incorporate agency protocols on what and how information is shared
- Develop a plan for handling a data breach or client grievance
- Determine the terms of the agreement; periodic review and/or renewal of the agreement will ensure the information remains relevant and up to date

Avoid Unintentional Information Sharing

Unintentional sharing of information is both the easiest and most common way that client confidentiality is compromised. Unintentional information sharing may occur due to a mistake, an oversight, or an incorrect assumption. Lax enforcement or misunderstanding of confidentiality policies and procedures are factors that may lead to unintentional information sharing.

Examples of Unintentional Information Sharing

- Conversations between co-workers who do not have the same 'need to know' status
- Conversations among co-workers in common or shared spaces
- Discussions with external service providers, landlords, or other external parties
- Inclusion of HIV/AIDS in agency/program name, slogans or mottos (see below)

- Lack of understanding or misinterpretation of confidentiality policies across agency or by individual staff members

It is important that an organization not use identifying information that could compromise a client's confidentiality in communications regarding the HOPWA program. If an agency or program name, logo, motto, or slogan identifies it as a provider of HIV/AIDS services, the organization should find ways to mask the information. For example, an agency might establish a separate entity with a separate name (e.g., Springfield Supportive Housing Program), designate a separate phone line for landlords to call, and/or set up a separate bank account with a generic program name.

Examples of Disclosure Risks from an Agency or Program Name

- Logos, slogans, and taglines
- Phone greeting (live and recorded)
- Caller ID
- Email imprint and signatures
- Staff titles
- Name badges and business cards
- Marketing materials such as signs, brochures, t-shirts, etc.
- Agency letterhead and envelopes
- Forms such as consent forms and leases
- Other printed materials
- Bank accounts
- Checks and invoices
- Tax filings[5]

Rural or small communities may face unique challenges to protect client confidentiality. In a small town, a local service provider, their staff, the location of their services, and the characteristics of their client populations may be well known. Clients may risk losing their privacy by accessing services from that provider. These providers should seek out service delivery methods that meet the needs of clients while protecting their privacy. For example, if an agency's office is well-known in the community, staff members could be available to meet clients at off-site locations.

[5] Agencies may be required to provide IRS documents to landlords that include the name of the organization. If this would compromise client confidentiality, the agency should consider removing references to HIV and AIDS from their agency name to protect themselves from breaches of confidentiality.

Best Practices to Avoid Unintentional Disclosures

- Ensure all staff understand confidentiality policies and procedures through regular staff training
- Require staff to sign confidentiality agreements
- Post notices about the importance of maintaining confidentiality throughout the office
- Direct staff to respond to third-party inquiries only after verifying that written client consent has been obtained
- Clarify information sharing policies with referring/referral agencies and other service and business partners
- Establish a separate entity under a generic name to perform certain functions
- Maintain distinct phone lines for certain purposes, such as receiving property owner calls
- Use non-HIV/AIDS specific agency names, program names and staff titles
- Avoid identifying the HOPWA program as a funding source when it would lead to disclosing the HIV status of clients served, including in housing assistance program materials of all sorts (e.g. leases, brochures, and webpages)
- Use an agency post office box to receive written correspondence
- Serve clients off-site as needed or when appropriate
- Do not issue housing assistance checks from bank accounts that reference "HOPWA", "HIV" or "AIDS" in the name

4.4 Reporting Client Data

HOPWA providers must report client and financial data to fulfill annual reporting requirements and complete reimbursements. They may also manage and report on funds from other sources, such as HUD's Homeless Assistance programs or the Department of Health and Human Services Ryan White Care Act. Each funding source has a unique set of reporting requirements; some sources require the use of a Grants Management System (GMS), such as a Homeless Management Information System (HMIS) for HUD's homeless programs or CAREWare for Ryan White Care Act funds. These systems may vary widely in their design, use, and purpose. Agencies should carefully consider how to report fiscal information along with sensitive client data and how to use a GMS while still protecting client confidentiality.

Provide Aggregate Client Data for HOPWA Reporting Purposes

All HOPWA grantees must complete and submit annual performance reports. Competitive grantees must submit the HOPWA Annual Performance Report (APR) form HUD-40100-C. Formula grantees must submit the HOPWA Consolidated Annual Performance and Evaluation Report (CAPER) form HUD-40100-D. HOPWA project sponsors must supply client demographic, output, and outcome data to their grantees who compile the data from multiple sources for

their own APR or CAPER. Client data shared for reporting purposes should always be in aggregate form. Personally identifying information is not required to fulfill reporting requirements and should not be included in any correspondence or documentation for reporting purposes.

Create Confidential Systems for Financial Reporting

HOPWA providers need to demonstrate that costs attributed to their HOPWA grant are allowable. Allowable costs are eligible, reasonable, allocable, and documented. Additional guidance on financial management is available in the *HOPWA Grantee Oversight Resource Guide* and *HOPWA Financial Management Online Training and Manual*. [6]

Financial reporting systems allow agencies to track costs and demonstrate that costs are allowable. Financial data, supporting documents, and the recording keeping system must allow for client information to be protected. This may also include the system of internal controls, staff time and activity tracking, and documentation, including case notes, calendars, client records, inspection reports, rent ledgers, or other information.

Any financial management or reporting system that reflects staff time and activities should use a code system to avoid the use of any personal client identifiers. Staff who set up such time and activity reporting systems should ensure that these systems are designed to enable staff to distinguish time spent working with different clients and on different activities. Unique identifiers should be sufficient to indicate eligible clients and activities without breaching confidentiality. Case notes and calendars are confidential documents that should be maintained in confidential files.

Use a Grants Management System (GMS) Appropriately

HOPWA providers who choose to participate in a Grants Management System (GMS) should consider the risks and benefits of sharing client information with other agencies. The use of a GMS as a means of capturing and sharing client information among providers could benefit clients by facilitating more organized and efficient care from each provider serving that client. Such systems can also expedite client referrals, track receipt of services, and allow measurement of client health outcomes. Disclosure risks, however, are important to understand and minimize while using a GMS or any internal or external electronic database. All providers participating within a single GMS should understand and uphold confidentiality practices in order to keep all information protected.

---

[6] The HOPWA Grantee Oversight Resources Guide is available online here: https://www.onecpd.info/resource/1003/hopwa-grantee-oversight-resource-guide/.
The HOPWA Financial Management Online Training and Manual is available online here: https://www.onecpd.info/training-events/courses/hud-hopwa-financial-management-online-training/.

Considerations for GMS Participation

- GMS-specific consent forms should be obtained
- Client information should only be shared for the limited purpose of serving that specific client
- Data sharing rules should be clearly defined and understood
- All participating staff members should receive training on when and with whom to share which information
- Participating agencies should develop a Participation Agreement outlining which information will be shared with other agencies and under what circumstances
- Participation Agreements should be amended as necessary
- HOPWA providers who participate in a HMIS should actively participate in the development, update, or ongoing review of the Continuum of Care data elements and data sharing policies and protocols

5. Monitoring

Confidentiality considerations during the monitoring process are important because the act of monitoring poses its own risk to confidentiality. HOPWA monitoring agents must review materials in the course of the monitoring process, such as HIV status documentation, housing plans and financial records. Monitors, therefore, will have access to confidential client information in order to verify that eligible services are being delivered to eligible clients.

The monitoring process will also include a review of confidentiality practices. The main purpose of this review is to verify that an agency has taken the proper steps to implement sound confidentiality practices. As a reminder, the language in CPD Notice 06-07[7], in reference to confidentiality, affirms that "grantees should conduct periodic monitoring of these procedures."

HOPWA grantees are responsible for monitoring their project sponsors to ensure that HOPWA funds are used for eligible clients and services and program activities are conducted in compliance with HOPWA and federal requirements. HUD's CPD Field Office staff also monitors HOPWA grantees and project sponsors from time to time as part of its responsibility to oversee grantees. HUD regulations 24 CFR 84.53(e) and 24 CFR 85.42(e) provide for HUD and its representatives, including grantees, the right to access documentation related to HOPWA awards for the purpose of making audits and/or examinations. Review of client records is, therefore, allowable without specific client consent. However, HOPWA-funded organizations

[7] The CPD Notice 06-07 is available online here: https://www.onecpd.info/resource/2781/notice-cpd-06-07-standards-hopwa-strmu-payments-permanent-housing/.

may choose to obtain permission from, or at a minimum, disclose to clients that their information may be reviewed for monitoring purposes. This permission or disclosure can be included on a consent form obtained at intake and can include language about precautions taken to maintain confidentiality.

Ideally, all agencies will work collaboratively throughout the monitoring process to ensure that monitoring can be successfully completed and confidential information remains protected. Additional guidance on monitoring is available in the *HOPWA Grantee Oversight Resource Guide* and *CPD Monitoring Handbook*.[8]

5.1 Grantee Monitoring Process

HOPWA grantees should inform each agency being monitored of their role as a monitor and set expectations for the monitoring process. HOPWA grantees should establish uniform procedures to ensure consistent monitoring and oversight of HOPWA funded activities. HOPWA grantees may choose to develop their monitoring protocols in conjunction with the agencies that will be monitored.

Best Practices for the Monitoring Process

- Establish written monitoring policies and procedures to ensure confidentiality
- Describe guidelines for documenting monitoring efforts
- Affirm the regulatory requirement for both confidentiality and monitoring in all grant and/or contractual agreements
- Train all staff on maintaining confidentiality during the monitoring process
- Establish a Confidentiality Agreement between the monitoring agent and the entity being monitored
    - Outline the expectations and responsibilities of each party
    - Identify how confidential information will be protected
    - Describe how breaches of confidentiality will be handled
- Limit the number of staff that review client files and file management procedures
- Examine the fewest number of client files necessary to achieve monitoring objectives
- Allocate a specific time period for reviewing confidential information
- Perform monitoring review in a private and secure location
- Do not leave confidential files unattended at any time
- Do not remove confidential information from the monitoring review location

[8] The HOPWA Grantee Oversight Resources Guide is available online here: https://www.onecpd.info/resource/1003/hopwa-grantee-oversight-resource-guide/.
The CPD Monitoring Handbook is available online here: http://www.hud.gov/offices/cpd/library/monitoring/handbook.cfm

    - Use unique identifiers or redact files if copies are needed beyond the on-site monitoring review period
    - Shred all notes taken during the monitoring process containing confidential information
    - Do not copy, fax, or email confidential information
- Document the monitoring process
    - Track who reviews information and what is reviewed
    - Note in the client file that it has been reviewed for monitoring purposes

5.2 Monitoring Confidentiality Practices

In developing a plan to monitor confidentiality practices, HOPWA monitors should focus on three key components: 1) review of confidentiality policies and procedures; 2) verification that policies and procedures are applied consistently; and 3) verification of effective staff training on confidentiality.

First, HOPWA monitors should evaluate whether the monitored entity has written policies and procedures that adequately address and protect client confidentiality. Comprehensive policies and procedures address issues such as obtaining client consent; collecting, storing and sharing data; and handling a data breach. A monitoring visit provides an opportunity for monitors to determine that an agency's policies and procedures are current, relevant, and comprehensive.

Second, HOPWA monitors should verify that these policies and procedures are being implemented effectively. Discussing the policies and procedures with agency program managers and staff is one way to verify that the agency's practices are clearly understood. HOPWA monitors should review available documentation demonstrating how an agency implements their policies and evaluate how data is collected and stored. This includes, for example, a review of client records and consent forms on file, examination of Participation Agreements, analysis of the data collection and storage processes, and assessment of the outcome of a data breach, if applicable. The best practices discussed throughout this document provide a framework for how to implement sound confidentiality procedures.

Third, HOPWA monitoring agents should review the plan for and implementation of staff training on confidentiality practices. This review should examine all training methods and/or materials that have been or will be used, recent and upcoming training schedules, and meeting agendas where confidentiality is discussed.

6. Addressing Data Breaches

For the purpose of this user guide, the term "data breach" refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information. The best way to prevent data breaches is to safeguard client data using the practices and guidance outlined in this document. However, even with effective policies and procedures in place to protect client confidentiality, data breaches may occur. HOPWA providers should have a written protocol for rapidly responding to data breaches to ensure steps are taken to limit the damage of a data breach and to notify those affected.

When devising a data breach protocol, agencies should be informed of any requirements set by funders and any applicable federal, state, and local laws. Most states have enacted legislation requiring notification of security breaches involving personal information. Additionally, HIPAA-covered entities are required to follow the breach notification provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) which was passed under the American Recovery and Reinvestment Act of 2009 (ARRA). Some laws impose fines or sanctions, if not properly followed. In addition, a provider that has had a data breach may face potential legal liabilities.

Several action steps are outlined below for HOPWA providers to respond to a data breach. Some of these steps may not be possible or necessary depending on the agency or type of data breach involved. Keep in mind that each of these steps is provided as a best practice for HOPWA funded agencies.

Health Information Technology for Economic and Clinical Health (HITECH) Act

The HITECH legislation applies to all HIPAA-covered entities. Key items include:

- Breach notification requirements for unauthorized use and disclosure of unsecured health information;
- Increased penalties for violations of Federal privacy and security laws; and
- Application of HIPPA provisions directly to business associates.

Additional guidance is available from the Department of Health and Human Services: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

6.1 Investigate and Secure the Data

In order to properly respond to any data breach, HOPWA providers should first identify and understand the scale and scope of what has taken place. Create a dedicated data breach response management team or designate a lead staff person to ensure a coordinated response to the incident.

Key Questions to Investigate a Data Breach

- How did the data breach occur?
- What data has been breached?
- What computer or record keeping systems have been compromised by the breach?
- Is the data breach ongoing?
- Where is the compromised data now?
- Who is affected by the data breach?

Various types of data breaches can take place and each will require a different response once fully investigated. For example, the improper disposal of paper documents will require different action steps than the unauthorized access of an agency's computer system. Additionally, once investigated, it may be determined that lost or stolen data was sufficiently encrypted to protect client confidentiality.

Once a data breach is discovered, take steps to mitigate any ongoing or future damage. The necessary steps to secure breached data will depend on what and how the data was breached.

Examples of How to Secure Data

- Attempt to retrieve and secure stolen or lost data
- Communicate the implications to any external recipients of breached data
- Disconnect from the Internet
- Shut down computer systems
- Reset passwords
- Limit staff or vendor access to data and records (especially if involved in the incident)
- Hire computer or security experts for assistance
- Identify legal or funding source requirements pertaining to data breaches

6.2 Notification and Prevention

After identifying whose information was compromised in a data breach and what data elements were included (e.g., name, age, date of birth, Social Security number, HIV/AIDS diagnosis), notify affected individuals in writing.

Best Practices for Data Breach Notification

- Provide dates of the breach and discovery
- Describe what happened and what information was involved
- Outline steps affected individuals should take to protect themselves
- Describe actions taken to investigate and remedy the breach
- Provide contact information for individuals to gain additional details or report harmful impacts of the breach (e.g., agency contact person, phone number, e-mail address, etc.)

Notifications are typically sent by first-class mail to the last known address of each affected individual. An email notification can be sent to affected individuals who agreed to receive notices electronically. If an affected individual is a minor, notice should be made to the parent or guardian. If the data breach included a large number of affected individuals, agencies may want to consider posting a general notice at office and program locations, on the agency website, or in print/broadcast media. Other parties that may also need to be notified include legal counsel, law enforcement, partner agencies, funders, insurance companies, or the media. After the data breach has concluded and all affected parties have been notified, review the incident, and take measures to avoid a similar future occurrence.

Best Practices to Prevent Recurrence

- Document the incident and response
- Re-train staff on confidentiality practices
- Revise agency policies or procedures
- Install new computer security systems

7. Conclusion

HOPWA providers will grapple with complex issues as they review their confidentiality policies, train staff, implement and use grant management systems, and employ strategies to protect clients' confidential information. Not only is protecting client confidentiality a HOPWA program requirement, it is also an essential practice consistent with the program's commitment to serve people living with HIV/AIDS in a manner that is fair, respectful and reflective of their needs. Without the necessary confidentiality protections in place, clients face an increased risk of stigma and discrimination, which may deter them from seeking care and needed services. Each agency should develop unique policies and procedures based on their particular program design and circumstances. There is no single definitive way to do this. The key component for all agencies is to continually make protecting private client information a top priority.

Appendix: HOPWA Confidentiality Checklist

Policies, Procedures, and Training

- ☐ Develop an agency-wide confidentiality policy
- ☐ Implement confidentiality policy with a set of standard operating procedures
- ☐ Plan regular training opportunities for all staff

Gathering Client Data

- ☐ Collect client data through private intake sessions
- ☐ Discuss privacy policies and obtain consent forms during intake and as needed

Storing Client Data

- ☐ Staff precautions: Limit the number of staff who have access to client data
- ☐ Hard copy precautions: Keep written records safe and secure
- ☐ Electronic precautions: Protect and limit access to electronic data

Sharing Client Data

- ☐ Ensure that client consent is obtained
- ☐ Discuss how to protect shared client data within the agency and with external partners
- ☐ Establish Participation Agreements with external agencies, as appropriate
- ☐ Avoid unintentional information sharing

Reporting Client Data

- ☐ Provide aggregate client data for HOPWA reporting purposes
- ☐ Create confidential systems for financial reporting
- ☐ Use a Grants Management System appropriately

Grantee Monitoring Process

- ☐ Establish uniform policies and procedures to ensure confidentiality
- ☐ Take precautions to protect confidentiality and limit exposure of identifiable information
- ☐ Train all staff on how to maintain confidentiality during a monitoring visit

Monitoring Confidentiality Practices

- ☐ Review agency confidentiality policies and procedure
- ☐ Verify that the agency consistently applies their confidentiality policies and procedures
- ☐ Verify that the agency regularly trains staff about confidentiality

Addressing Data Breaches

- ☐ Investigate the data breach and appoint a team or individual to lead effort
- ☐ Take immediate action to secure breached data
- ☐ Notify affected and appropriate parties
- ☐ Take steps to prevent future data breaches