# POLICY AND PROCEDURE NOTICE: PPPN-007
## CONFIDENTIALITY

**Summary and Purpose of PPPN:** To guide the administration of the Ryan White Part A Program in ensuring client confidentiality and maintaining the privacy and security of individually identifiable health information.

**Authority**:

- Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104-191, 110 Stat. 1936, enacted August 21 1996)
- 45 CFR Parts 160 through 164 and 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e) Standards for Privacy of Individually Identifiable Health Information
- Social Security Act § 1171-1179
- OCGA § 24-9-42
- OCGA § 24-9-47 Disclosure of AIDS Confidential Information
- OCGA § 24-12-1
- OCGA § 24-12-2
- OCGA § 24-12-10
- OCGA § 24-12-11
- OCGA § 24-12-13
- OCGA § 24-12-14
- OCGA § 24-12-20
- OCGA § 24-12-21
- OCGA § 37-3-166
- OCGA § 31-7-6
- OCGA § 37-7-166
- OCGA § 31-2-8
- OCGA 31-33-2 (a)(1)(A)
- Georgia Rules and Regulation 290-9-7-18

**Cross-reference: PPPN-010 Data Management Subrecipient Internal Policies**

**Policy and Procedure**:

The Ryan White Part A Program is committed to protecting the confidentiality of personal health information in accordance with the Federal Health Insurance Portability and

Accountability Act of 1996 (HIPAA)[1] and federal, state, and local privacy laws, rules, and regulations. An individual's health information should only be disclosed to people who have a legal right to receive it, whose identity has been verified, and whose authority to receive it has been verified. Health information shall not be disclosed or made available to unauthorized persons, and precautions shall be taken to ensure that health information is not disclosed to unauthorized persons. **Note: These standards apply even if a patient is deceased.**

1. Limitations in release of Protected Health Information (PHI): The HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, and electronic, etc. Furthermore, only the minimum health information necessary to conduct business is to be used or shared.

2. Subrecipients must abide by all state and federal laws, rules and regulations and County policies respecting confidentiality of an individual's records. Subrecipients must not directly or indirectly disclose any information concerning any individual to any unauthorized person without the written consent of the individual, employee, client or responsible parent or guardian.

   Examples of direct and indirect disclosure:

   - **Direct disclosure:** any verbal or written communication with a third party that discloses the name or other identifying information (e.g. social security number) of an HIV+ individual and the individual's HIV+ status
   - **Indirect disclosure:** any verbal or written communication with a third party that discloses the name or other identifying information (e.g. social security number) of an HIV+ individual, such that the third party can reasonably infer that this individual is HIV+.
     - Disclosure of client identifying information in the course of seeking services for the client from a service provider that serves primarily HIV+ persons
     - Disclosure of client identifying information in conjunction with disclosure of the name of the agency providing the information when this agency serves primarily HIV+ persons, regardless of whether or not the name of the agency directly reveals its target population.

[1] Among other things, HIPAA defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information as well as outlining numerous offenses relating to health care and sets civil and criminal penalties for violations.

- Disclosure of identifying information in conjunction with disclosure of the name of the individual providing the information when this individual is well-known in the medical and/or social work community as an HIV provide.
- Leaving a return number on an answering machine, voice mail or pager that, when called by another household member, could result in the disclosure of protected information (e.g. the agency receptionist answers the phone, "Hello, Sunshine AIDS Services" before transferring the call).
- Written correspondence to the client containing a revealing return address (e.g. "from Sunshine AIDS Services"), e-mail address, etc. that could be viewed by another household member.

3. Subrecipients must provide notification of the agency's Confidentiality Policy/HIPAA Policy and Statement of Health Information Practices to all clients rendered services in accordance with your Contract. Client files shall include an affirmation signed by the client indicating receipt of information.

4. **Consents to Release/Exchange Information**: A copy of a client's medical record or protected health information may be released to any person or entity designated in writing by the client if the client is a competent adult, or by the custodial parent(s) of a minor, the legal guardian of a minor, or a person to whom legal custody has been given by order of a court. Records are produced according to the client's authorization will bear notice to the recipient concerning restrictions on further use or disclosure by the recipient.

   Except as noted below, a subrecipient agency will obtain the informed written consent of the client or the legally responsible individual prior to releasing or exchanging PHI with a third party any information that directly or indirectly reveals the client's HIV+ status. Exceptions:
   - A medical (physical, mental or emotional) emergency, in which case information may be released to medical personnel or the appropriate regulatory agency (e.g. Adult Protective Services) only, after verbal consent—if possible—is obtained from the client or legally responsible individual
   - A court order or subpoena
   - All consents to release/exchange information must contain the expiration date of client authorization (or expiration event) that is no longer than 2 years from the date of original signed consent.
   - All consents to release/exchange information must contain the names of the individuals and/or agencies to whom the information may be released.
   - There is no limit to the number of persons and/or agencies that can be listed on a single consent form. However, any consent form containing a pre-printed list of agencies must include an option for clients to limit their consent to only the agencies

of their choice by drawing a line through the agencies they do not want and initialing it.

- All consents to release/exchange information must contain the type(s) of information that may be released and the purpose or reason for the release.
- Consents to release/exchange information must be separate from the consent for services.
- All sections on the consent to release/exchange information form must be completed prior to the form being signed by the client. Under no circumstances should a client be asked to sign an incomplete or blank consent form. All unused lines must be crossed out. Furthermore, no additional agencies or individuals may be added to the consent form after the date of original signature; a new form must always be used for any additions.
- Consent to release/exchange information is not required for verbal or written communications that do not involve the disclosure of client identifying information (e.g. calling service providers to inquire about service availability without giving a client's name or social security number).
- The client record must contain documentation of each instance of disclosure of confidential information, including the date, nature and purpose of the disclosure, the name of the agency or individual to whom the information is disclosed, and the signature of the agency representative disclosing the information.
- The agency will obtain a signed "Statement of Confidentiality" from all officers, employees and/or volunteers who require access to client records in order to perform their duties. The statement will indicate that the undersigned agrees to respect the confidentiality of all agency clients.
- Clients must be allowed to withdraw their consent to release/exchange information with any individual or organization at any time.

5. **Records Administration**:
   - All client records and other records containing client-identifying information are confidential and must be housed in file cabinets and drawers with working locks with limited access. These should be locked securely during all non-working hours and during working hours when the records are not in use. Double-locking (i.e., room and file cabinet) is preferred.
   - File cabinets and drawers containing confidential records must be located in areas of the agency facility that are not freely accessible to clients or the general public.
   - Rooms containing confidential information must not have windows that could allow easy entry into the room or easy viewing of the information from outside.
   - Clients and other agency visitors will not be left unaccompanied by agency staff in an office or any portion of an agency facility containing unlocked confidential records.
   - Only agency staff and/or volunteers who have signed a "Statement of Confidentiality" will be allowed access to confidential records.
   - Confidential records will be re-filed as soon as possible after use.

- Confidential record documents, i.e. any documents containing client-identifying information, will be shredded prior to disposal using a commercial-grade shredder with a crosscutting feature.
- Except under very unusual circumstances (e.g. a move to a new facility, archiving), confidential records will not be removed from the agency facility in which they are housed. Confidential records will not be taken on home or field visits or taken home by agency staff.
- Adult Client Health Records must be maintained by the agency for no less than 10 years following the last date of service to the client. O.C.G.A. 31-33-2 (a)(1)(A) states that adult health records are to be kept by the healthcare provider for a period of 10 years.
- Child Client Health Records must be maintained by the agency for no less than 10 years after client reaches age of majority (18). While the Georgia Rules and Regulation 290-9-7-18 states that medical records of minors must be kept at least until 5 years after the client reaches the age of majority (18), DPH policy is that the legally preferable retention period would be to match that of adult health records, i.e. to keep minors' records for 10 years after they reach age of majority.
- Stored confidential documents must be clearly marked as containing confidential information. Containers must not be labeled as having TB, HIV, or STD documents.

6. **Fax cover sheets** must have the appropriate language and state "Confidential." This language must include:

   HIPAA Privacy Rules require covered entities to safeguard certain Protected Health Information (PHI) related to a person's healthcare. Information being sent to you may include PHI, after appropriate consent, acknowledgement, or authorization from the patient or under circumstances that do not require patient authorization. This transmission may contain material that is confidential under Federal law and Georgia Statutes, and is intended to be delivered to only the named addressee. Unauthorized use of this information may be a violation of criminal statutes. You, the recipient, are obligated to maintain PHI in a safe and secure manner. You may not re-disclose this patient information without additional patient consent or as required by law. Unauthorized re-disclosure or failure to safeguard PHI could subject us, or you, to penalties described in federal (HIPAA) and state law. If you, the reader of this message, are not the intended recipient, please notify us immediately and destroy the related message.

7. **Electronic Files:** The use of electronic files to gather and collect client information requires specific precautions to avoid a breach of confidentiality and protect the client's right to privacy.
   - Computer monitors must be positioned to prevent unauthorized viewing.

- All computers, including laptops and tablets, that access and store confidential information must be password protected; and the data must be encrypted in accordance with information security policies, protocols, and procedures.
- Laptops may be used for storing and accessing HIV/AIDS information with client identifiers only if the computer is password protected and files are and files are encrypted or password protected.
- Laptops containing confidential information must be returned to the secured area at the subrecipient facility at the end of the working day and never stored in an unsecured, unauthorized area. This directive includes storing laptops in the employee's car, car trunk, or home unless there is prior supervisory approval.
- Deleting files from a computer hard drive is not necessarily sufficient if the computer is to be stored. Hard drives must be wiped clean. If you are unsure how to do this or what it means, consult with your Information Technology staff.

8. **Computer Workstations**:
   - Computer workstations with access to confidential information must be located in a secure area. A secure area must provide at least one level of physical security, although it is preferable that workstations with access to protected health information be kept behind two levels of physical security.
   - Computer screens that display confidential information must not be readily observable by non-authorized users in the office area. Security screens may be installed on computer monitors to prevent viewing of information by anyone other than the operator.
   - Computers that access confidential information must be password-protected at the Windows login level; a password-protected screensaver program must be installed that activates after a few minutes of inactivity by the user.
   - All network/computer passwords are to be at least eight characters long and should be a combination of letters, characters, and numbers.
   - Network/computer passwords must expire based on current password guidelines.
   - Temporary passwords must expire once the user generates a password.
   - Users must never share their passwords.
   - Computer workstations must be locked (Ctrl/Alt/Delete - Lock Workstation) whenever a workstation is unattended.
   - Internet Control Message Protocol (ICMP) should not allow "Redirect Services" to devices (e.g., smartphones, tablets) not authorized by network administrators.
   - Network services should not allow "remote desktop" access by non-network users.
   - Confidential data must not be accessed on any computer that is not secure.

9. **Electronic Data:**
   - Network drives, which contain confidential information, must have controls in place that prevent unauthorized user access.

- In the case of remote access from approved home-based computing devices, firewall, anti-adware/spyware, and anti-virus protection, appropriate security patch levels must be installed, active, and maintained by the remote user.
- Electronic data must be held in a technologically secure environment; the number of data repositories and the number of permitted users must be kept to a minimum.
- Personal computers or personal electronic media should not be used for data storage. Data Storage devices must be issued by the agency. Only an agency-issued device, internet service provider (ISP), or personal network equipment may be used for internet connectivity.
- Confidential information must either be stored on a computer which is not connected to a network (i.e., stand-alone computer) or on a secure drive of a secure network (e.g., network with restricted access and/or firewall protection). An agency must have properly configured firewalls installed on computers to be used outside of the agency's secure network.
- Confidential information should never be stored on the hard drive of any computer connected to a local or wide area network (WAN). PHI should never be stored on a device that is connected to the internet, either directly or indirectly, outside the agency firewall.
- Agency issued computers must be configured to prevent installation of software by persons other than agency IT staff.
- Stored datasets containing PHI must be encrypted using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES) FIPS-197 (PDF) [U.S. National Institute of Standards and Technology] and stored either on a stand-alone computer or on a secure drive. (Data at Rest standard)
- Confidential data should not be stored on wireless handheld devices. In the event there is no alternative to local storage, all sensitive, confidential, and restricted personal information, including PHI, must be encrypted.

See also: Georgia STD Data Security and Confidentiality Policy
https://sendss.state.ga.us

## Verification:

1. Review of subrecipient Confidentiality Policy/HIPAA Policy and Statement of Health Information Practices.
   - Review client charts/records/files for presence of affirmation signed by the client indicating receipt of Confidentiality Policy/HIPAA Policy and Statement of Health Information Practices information.

- Review client records to verify signed consent forms and to validate each instance of disclosure of confidential information, including the date, nature and purpose of the disclosure, the name of the agency or individual to whom the information is disclosed, and the signature of the agency representative disclosing the information.

2. Examine personnel files for presence of signed "Statement of Confidentiality" from all officers, employees and/or volunteers who require access to client records in order to perform their duties.
   A. Validate that the statement indicates that the signatory agrees to respect the confidentiality of all agency clients.

3. Review agency Business Associate Agreements to ensure agreements are in place with all Part A subrecipients.

4. Review records administration policies (including file retention) and verify protection of records.

5. Review fax cover sheet for HIPAA language.

6. Verify protection of electronic files: positioning of monitors, password protections, encrypted files on laptops, and process for checking-in laptops at day's end.

**Approved: October 2016**

**Reviewed: April 2021**