POLICY AND PROCEDURE NOTICE: PPPN-010
DATA MANAGEMENT SUBRECIPIENT INTERNAL POLICIES

Summary and Purpose of PPN: 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 through data management policies and procedures.

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
- Fulton County Ryan White Part A Contract/Agreement

Cross-reference: PPPN-007 Confidentiality

Policy and Procedures:

1. Subrecipients must develop written policies and procedures on data security and confidentiality; review policies and procedures at least annually; revise them as needed;

and ensure their review by and accessibility to all staff members and volunteers having authorized access to confidential individual-level data.

Policies must detail the step-by-step process of the agency's internal procedures for ensuring e2Fulton and hard copy data files are secure with assignment of staff responsibility for monitoring data security clearly identified.

2. Subrecipients must designate a person or persons to act as the Overall Responsible Party (ORP) for the security of health data the program collects or maintains, and ensure that the ORP is named in any policy documents related to data security. The purpose of naming an ORP is to increase program accountability for data security. The ORP should have the authority to modify programs and policies to meet the standards in this document. The ORP can be selected from the program, department, or agency level. The agency's organizational structure might demand designating more than one person as ORP (i.e., an ORP panel). The ORP(s) may also choose to have data releases or proposed data sharing activities reviewed by a group of designated individuals to facilitate the review process and ensure the risks and benefits of the proposed activities are considered and make recommendations.

   The specific agency staff position designated as ORP must be identified and listed with the Fulton County Ryan White Part A Program Data Manager.

3. Subrecipients must ensure that data security policies define the roles and access levels of all persons with authorized access to confidential public health data and the procedures for accessing data securely. Access to surveillance data needs to be planned. The number of people with access to identifiable information should be kept to a minimum, and de-identified data should be used for routine analyses whenever possible. Operational security procedures should be devised to minimize the number of people with access to confidential data. Written procedures should specify how to obtain authorization for access to both Personally Identifying Information (PII) or Protected Health Information (PHI) and de-identified data.

4. Subrecipients must ensure that data security policies require ongoing reviews of evolving technologies and include a computer back-up or disaster recovery plan. Because the technology used to secure data is constantly evolving, information technology and security professionals should be included in the development and review of data security policies and procedures.

5. Subrecipients must ensure that any breach of data security protocol, regardless of whether personal information was released, is reported to the ORP and investigated immediately. Any breach that results in the release of PHI/PII to unauthorized persons

should be reported to the ORP, to the Part A Recipient, and if warranted to law enforcement agencies. The data security policy should include procedures for reporting suspected breaches, including who to notify about a suspected breach. Staff members should be familiar with the program's definition of a security breach. Staff members should review procedures during annual security training. A log of security breaches and lessons learned during investigations of breaches might be useful in revising security policies. If PHI from a federally supported system were to be released to, or stolen by, unauthorized persons that breach must be reported to federal security officials within one hour of its discovery.

6. Subrecipients must ensure that staff members with access to identifiable public health data attend data security and confidentiality training annually. All staff members (including IT personnel, contractors, and mail room and custodial staff) require generic security awareness training to ensure and support a culture of confidentiality, but staff who have access to PII require additional training specific to their responsibilities and level of authorized access to PII. Training should cover:
   - Personal responsibilities
   - Procedures for ensuring physical security of PII
   - Procedures for electronically storing and transferring data
   - Policies and procedures for data sharing
   - Procedures for reporting and responding to security breaches
   - Review of relevant laws and regulations

   All staff should have documentation of completion of their training. Programs are responsible for maintaining this documentation in their personnel files.

7. Subrecipients must require all newly hired staff members to sign a confidentiality agreement before being given access to identifiable information; require all staff members to re-sign their confidentiality agreements annually. All staff (including IT, mail room, and custodial staff) should sign a nondisclosure or confidentiality agreement stating that the employee agrees not to release PII to any unauthorized persons. The agreement should be maintained in the employee's personnel file. A confidentiality agreement should be required before assigning passwords or keys that allow access to PII. Policies and procedures should address staff out-processing and relinquishment of authorized access.

8. Subrecipients must ensure that all persons who have authorized access to confidential public health data take responsibility for 1) implementing the program's data security policies and procedures, 2) protecting the security of any device in their possession on

which PII are stored, and 3) reporting suspected security breaches. The data security responsibilities of staff members should be incorporated into their confidentiality agreements and reviewed during annual training. Supervisors should consider including security-related questions in annual performance reviews as a way of gauging staff members' understanding of their data security responsibilities.

Responsibilities of persons with authorized access to PII include but are not limited to:

- Protecting keys, passwords, and codes that would facilitate unauthorized access to PII
- Taking appropriate action to avoid infecting computer systems with viruses and other malware
- Protecting computers and devices from extreme heat and cold
- Protecting mobile devices and storage media from loss or theft
- Appropriate use of personal computers and storage devices
- Appropriate removal of data from secure facilities

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

See also: Protected Health Information and Personal Identifying Information
http://ora.research.ucla.edu/OHRPP/Documents/Policy/6/PHI_PII.pdf

Verification:

- Review subrecipient written policies and procedures regarding data security and confidentiality.
  A. Validate that the policies and procedures consistent with the standards in this document.
  B. Validate that the policies and procedures available and accessible to program staff.
  C. Validate that staff are trained in the policies and procedures and alerted to any revisions.
  D. Validate that an ORP been designated and named in all relevant policy documents.
  E. Validate that the ORP has authority to modify data security policies and procedures for compliance with the standards in this document.
  F. Validate that authorized access granted based on the data user's need to know.
  G. Validate that the number of persons with access to PII is kept to a minimum.
  H. Validate that persons with technical expertise in information and system security been consulted to ensure that data security policies and procedures are adequate.
     - Verify if policies and procedures include a disaster recovery plan.
  I. Verify procedures in place to respond to breaches in data security.

- Verify if the data security policy identify the person to be notified if a breach is suspected.
- Verify if staff members are familiar with the program's definition of a security breach.

J. Verify if security training is required for new staff members and annually for all staff members.
   - Are there specific modules related to job responsibilities? For example, mail room and custodial staff would have different training components based on job duties and likelihood of access to confidential material.
   - Does the training cover the standards in this document?
   - Does the training include a review of physical and electronic data security procedures, confidentiality procedures, and release and sharing procedures on an ongoing basis?
   - Is attendance at the training sessions documented?
   - Are training materials updated as needed?

K. Verify that all staff members are required to sign a confidentiality agreement before they are granted access to PII.
   - Are the data security responsibilities of staff members outlined in their confidentiality agreements?
   - Are these responsibilities reviewed annually?
   - Do staff members know how, and to whom, to report suspected security breaches or instances of unauthorized access? Are they familiar with the criteria for reporting and investigation?

Approved June 2016

Reviewed: March 2021