

**Georgia Department of Public Health  
STD Office**

# **Georgia STD Data Security and Confidentiality Policy**

**Revised November 2014**



# Table of Contents

---

## **Program Policies and Responsibilities** .....

Purpose	Overall responsible person (ORP)
STD surveillance data collection	Levels of access of STD PHI
Personally identifiable health information (PHI)	Breach of confidentiality
Confidentiality guidelines	
Confidentiality agreement	

## **Physical Security** .....

Building/workstations	Paper record storage
Offsite workstations/telework	Record retention
Field work	Shredding
Mail	Physical security of servers

## **Data Security** .....

Computers and laptops	Retirement of hard drives
Use of hand held devices	Printing
Email	Data sharing and release
Telephone	Data suppression
Fax	Routine reporting to CDC

## **Appendices**

Georgia Department of Public Health, Confidentiality of Personal Health Information and Compliance with HIPAA (Policy# GC-09013)

Georgia Department of Public Health Personal Health Information Security Incident Response Protocol (Form GC-09013E)

Georgia Department of Public Health Policy #IT-13002 Information Security Program Policy

Georgia Department of Public Health Policy #HR-03403 (Work Away Policy)

Georgia Department of Public Health Policy #CO-12007 Data Request Policy

Georgia Department of Public Health Policy #CO-12009 Data Standards Policy and Procedures

## Program Policies and Responsibilities

### Purpose:

- The purpose of this document is to standardize STD data security policies and procedures when collecting, transmitting, storing and maintaining confidential STD information.
- All staff (state and district), contractors, interns, and volunteers with access to the STD SendSS Case Management are required to adhere to this policy in order to maintain access.
- All individuals who have authorized access to confidential STD information take responsibility for: 1) implementing these data security policies and procedures, 2) protecting the security of any device in their possession on which confidential STD information are stored, and 3) reporting known or suspected security breaches.

### STD surveillance data collection:

- STD data are collected for public health purposes only.
- The minimum data are collected that satisfy public health surveillance needs.
- Data collection should lead to reduction in morbidity through targeted public health interventions.

### Personally health information (PHI):

- PHI is defined as any information about an individual that can be used to distinguish or trace an individual's identity.
- Cross-tabulations of case characteristics and rates, if sufficiently specific and if numbers are small, may also be considered PHI.
- The STD Office shall collect personally identifiable data only when necessary and use non-identifiable data whenever possible.

### Confidentiality guidelines:

- These guidelines serve as the overall policy for all STD public health activities in the state of Georgia.
- These guidelines describe the policies and methods used to safeguard the confidentiality of STD surveillance information.
- These guidelines are reviewed and updated annually or as needed by the STD Surveillance Manager in response to changing technologies, personnel, or policies.
- These guidelines cover CDC-funded activities of the STD Office. These guidelines are intended to be in compliance with the CDC *Data Security and Confidentiality Guidelines*.

<http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf>

*Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action.*

U.S. Department of Health and Human Services;  
Centers for Disease Control and Prevention; Atlanta, GA; 2011.



- These guidelines are intended to supplement the *Georgia Department of Public Health, Confidentiality of Personal Health Information and Compliance with HIPAA (Policy# GC-09013)*
- These guidelines should be considered a minimum standard. There may be scenarios not covered by these guidelines where staff and STD Program Coordinators will need to exercise good judgment about security and confidentiality of PHI and may apply more stringent standards.

Confidentiality agreement:

- All new staff (state and district), contractors, interns, and volunteers needing access to STD SendSS Case Management must sign the STD Confidentiality Agreement prior to being granted access.
- All individuals with access to STD SendSS Case Management must receive training and sign the STD Confidentiality Agreement annually to maintain access.
- By signing the STD Confidentiality Agreement, individuals agree to abide by the *Georgia STD Data Security & Confidentiality Policy*.
- Signed STD Confidentiality Agreements should be kept by STD Program Coordinators. A copy of the signed agreements should be sent to the state office.

Overall responsible person (ORP):

- The overall responsible party (ORP) accepts responsibility for implementing and enforcing STD policies and procedures related to the security and confidentiality of SendSS data.
- The ORP has the responsibility of reporting and assisting in the investigative breach process.
- The ORP must certify annually that DPH is in compliance with CDC guidelines.
- The ORP is Michelle Allen, State STD Director. Upon the vacancy of the State STD Director position, the STD Surveillance Manager, currently Latasha Terry, will be the interim ORP.

Levels of access to STD PHI in SendSS:

- District/State View Only – Permission grants ability to view patient records without the ability to edit a record.
- DIS – Permissions include the ability to search and edit patient records.
- District Clerk/ Surveillance – Permissions include all of the above and the ability to delete field records and assign new ELR or incoming OoJ field records to staff.
- District Supervisor – Permissions include all of the above and the ability to submit field records/ interview records to the state.
- Regional Consultant – Permission includes the same permissions as District Supervisor as well as the ability to accept or return field records/interview records that have been submitted to the state for review.
- State Clerk – Permissions include ability to search and edit patient records. It may also include the ability to delete field records, assign new ELR, and initiate incoming OoJ field records to health districts.

- HIV Surveillance – Permission grants the ability to view any patient record without the ability to edit a record. It may also include access to HIV Record Search Requests and update historical information.
- State Administration – Permissions include all of the above as well as the ability to delete morbidity, merge records/events, add new providers/laboratories, reset SendSS accounts, review pending reports, and switch to another user for technical assistance only.

Breach of confidentiality:

- Breach of protocol – any violation of the confidentiality guidelines.
- Breach of confidentiality – any unauthorized use or disclosure of PHI.
- The STD Office will adhere to the *Georgia Department of Public Health Personal Health Information Security Incident Response Protocol (Form GC-09013E)*.
- All staff (state and district), contractors, interns, and volunteers must take responsibility for reporting any known or suspected security breaches to their STD Program Coordinator immediately.
- STD Program Coordinators must report any known or suspected security breaches to the ORP immediately.
- Breaches will be investigated and documented in the breach log.
- The CDC will be notified if a breach of confidentiality occurs resulting in the disclosure of confidential information.

## Physical security

### Building/ workstation:

- All staff (state and district), contractors, interns, and volunteers with authorized access must display identification badge at all times.
- Work areas should only be accessible to authorized staff.
- All visitors must be escorted by authorized staff at all times while inside the work area.
- All staff (state and district), contractors, interns, and volunteers are responsible for safeguarding confidential materials in their workstation cubicle.
- All paper documents containing STD PHI must be locked in desk or filing cabinet when not in use.
- All computers used to access STD SendSS must be in a secure area.
- STD PHI should only be entered into approved patient registry.
- If visitors enter the cubicle when data are being entered, the monitor should be turned off if PHI is visible by others and documents turned over.
- Computers and laptops must be locked or logged off when not in use (press the *Ctrl+Alt+Delete* at the same time, then at the Windows Security select 'Lock Computer').

### Offsite workstations/ telework:

- Staff must comply with *Georgia Department of Public Health Policy #HR-03403 (Work Away Policy)* when working from any offsite location.
- STD Program Coordinators must authorize any staff to work at an offsite location including telework.
- Security requirements for offsite locations are the same as normal workstations.
- DPH laptops should be secured in lockable cabinets or computer bag when not in use.
- Lockable cabinets or computer bags should only be accessible to DPH staff when storing STD PHI not in use. Locked cabinets or other secure bags must not be shared with or accessible to other household members.
- PHI that are no longer needed offsite must be returned to normal workstations.
- Internet connection via Wi-Fi should not be public Wi-Fi and must be password protected.
- Personal computer, laptop, fax machines, copiers, or printer must not be used. These machines may have hard drives that retain images of materials processed.

### Field work:

- STD Program Coordinators should always be aware of the use of STD PHI in the field. Staff should consult with their STD Program Coordinator before using PHI in any new ways.
- STD Program Coordinators should annually review with staff the use and security of PHI.
- Staff working with documents containing PHI in the field should return the documents to a secure area by close of business. Prior approval is required if not able to do so.
- Documents containing PHI must be stored in a locked computer bags or other storage container when information is not in use or unable to return documents to a secure area at the close of business.

- Loss of PHI or other breach must be reported to the STD Program Coordinator immediately.
- All staff (state and district), contractors, interns, and volunteers should take precautions to minimize risk of a breach of confidentiality when traveling to and from sites.
- Documents with line lists or supporting notes should contain the minimum amount of potentially identifiable information necessary and, if possible, potentially identifiable data should be coded (disease codes, dispositions, etc.) to prevent inadvertent release of PHI.
- Medical record reviews must be conducted where confidentiality can be assured.
- PHI extracted from medical records must be the minimum necessary and limited to that required for case management and field investigations.
- PHI should not be recorded in calendars, planners, or notes unless crucial for case management.
- PHI should not be entered into personal laptops, personal mobile devices, personal cell phones, personal tablets or other personal electronic devices.
- Preferably, PHI should not be left unattended in a vehicle. If it is determined that the safest course of action is to leave PHI in a vehicle, it should be kept in the trunk. If there is no trunk, it should be kept out of view under a seat or in a bag or container.
- If PHI need to be taken to a staff person's residence, PHI should be secured until they can be returned to the office. No one, including family members, should have access to PHI.

Mail:

- All outgoing mail containing PHI must be marked "CONFIDENTIAL".
- All mail should be collected promptly each day.
- Laboratories and providers sending mail containing STD PHI to the state office should use the following address:

Georgia Department of Public Health  
STD Office  
2 Peachtree St, NW Suite 13-463  
Atlanta GA 30303

**Envelope should be marked "CONFIDENTIAL."**

- When mail is inadvertently sent to the wrong program, it should be forwarded immediately. Mail should be forwarded in sealed interoffice envelopes to the appropriate program.
- Unprocessed mail should be stored in a locked cabinet until it can be processed.

Paper record storage:

- All paper documents containing STD PHI should be stored in a secure, locked area.
- Once STD cases are entered, paper records should be stored in either lockable filing cabinets or in boxes in a designated locked area.
- Access to STD locked areas should be limited to appropriate staff. Keys to locked areas must be controlled by designated staff.

Record retention:

- STD paper reports are retained for a minimum of one year
- Electronic records are kept indefinitely as part of STD surveillance registry (SendSS).

Shredding:

- Paper containing PHI must be shredded before disposal.
- Shredders should be crosscutting shredders.
- Personal shredders in cubicles are appropriate for low-volume shredding jobs.
- When a shredding vendor is used, an STD staff member must observe the onsite shredding process.

Physical security of the servers:

- STD SendSS database:
  - Located on GA DPH servers.
  - DPH servers are the responsibility of the IT Section and are stored in a locked room with proximity card access. The floor also has proximity card access.
  - DPH IT adheres to *Georgia Department of Public Health Policy #IT-13002 Information Security Program Policy*

## Data security

### Computers and laptops:

- Computers and laptops must be locked or logged off when not in use (press the *Ctrl+Alt+Delete* at the same time, then at the Windows Security select ‘Lock Computer’).
- Computer screens must not be readily observable by unauthorized people.
- When possible, all computers and laptops used to view STD PHI should have privacy screen on monitors to prevent unauthorized viewing.
- Computers and laptops used to access STD PHI must be password protected.
- Passwords must not be shared.
- Storage of passwords is discouraged; however, if passwords are stored, they must be encrypted.
- Staff may use DPH laptops at authorized offsite workstations.
- STD PHI must not be stored on the hard drive of any computer or laptop.

### Use of removable storage devices, smart phones, tablets, or other hand-held devices:

- Personal phones, tablets, or other unspecified devices should not be used to access, record, or photograph STD SendSS.
- Government issued tablets are acceptable to access STD SendSS.
- All confidential information placed on a removable storage device must be encrypted, using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and password protected. The password must not be stored with the device.

### Email:

- Email should not be used to send STD PHI.
- Email can become publicly available under the Freedom of Information Act.
- If email is received which includes STD PHI, the following steps should be taken: delete the email containing the PHI. If responding to the email, remind the sender not to send PHI through email.

### Telephone:

- Staff must only discuss patient information with authorized person during telephone conversations and should minimize the use of patient names, when possible. Every effort should be made to protect confidentiality of case information.
- When the identity of a healthcare provider requesting medical information on a patient is not known, ask the caller to submit the request in writing.
- For state office surveillance staff communicating with surveillance staff in other states, refer to CDC’s *STD Project Area Point of Contacts with Data Sharing Protocols for using Interstate Communication Control Records*.

Fax:

- STD PHI being sent using a fax machine must be sent with a cover sheet which include name, contact information for sender and recipient, confidentiality disclaimer statement and instructions on what to do if the document is received in error.
- Cover sheets should not contain the word STD/HIV.
- General DPH fax cover sheets may be used.
- Fax machines used to send or receive PHI must be located in a secure area.
- Fax machines should only be not used at a minimal to send or receive PHI.
- All STD/HIV related information should been removed or converted to a disease code.
- Anyone sending a fax must confirm that the information faxed was received by the intended recipient.
- The fax machine should be checked each night to ensure that PHI are not in the tray.

Retirement of hard drives:

- IT will destroy or erase hard drives for all computer, laptop and fax machines used by the STD Office when scheduled for retirement.

Printing:

- STD PHI must only be sent to government issued printers.
- Confidential print jobs should be sent to a printer within the program if available. A centralized printer may also be used as an alternative. Staff should ensure that confidential files are not printed out at the centralized printer unattended.

Data Sharing and Release:

- The STD Office will adhere to the *Georgia Department of Public Health Policy #CO-12007 Data Request Policy* and the *Georgia Department of Public Health Policy #CO-12009 Data Standards Policy and Procedures* with data requests.
- All data requests must be approved by the State STD Director before release of STD data.
- Data must only be released by individuals authorized by the State STD Director.
- Datasets used for analysis should include the minimum elements necessary and should not include PHI unless necessary.
- STD data release is limited to those with a justifiable public health need except where required by law.
- Data that is transmitted to other programs or outside agencies by electronic file (CD or other transport medium) must be secured.
- STD data in SendSS is considered provisional data. The release of STD SendSS data is discouraged.

Data suppression:

- Aggregate data tables are available at the state, county, and town/city level. Information for some geographic areas may not be released if there are concerns about low cell size or small numerators/denominators.
- Tables resulting in cell sizes of five or less may only be released to districts for programmatic use only.

Routine reporting of surveillance data to CDC:

- STD data are reported weekly to CDC via NETSS.



**Georgia Department of Public Health  
Division of Health Protection  
STD Office  
Data Security and Confidentiality Policy Agreement**

I \_\_\_\_\_, as an employee, contracted employee, intern, volunteer, or visiting professional, have reviewed and will adhere to the Georgia STD Data Security and Confidentiality Policy in order to gain or maintain access to STD SendSS Case Management. I understand I will have access to privileged patient information and understand my responsibility in the handling of confidential information. I understand that intentional or unintentional violations are subject to disciplinary action which might include, but not be limited to, termination of SendSS access or privileges, termination of employment or prosecution. I understand that I am bound by this policy, even upon resignation, termination, or completion of my activities.

I understand that I will have access to information by which the identity of a patient can be determined, either directly or indirectly. Example of this may include:

- Patient demographics: date of birth, address, phone, social security number, etc.
- Patient medical records: diagnosis, treatment, living arrangements, social history, lifestyles, sexual orientation, finance, etc.
- Exposure to an STD.

I agree to:

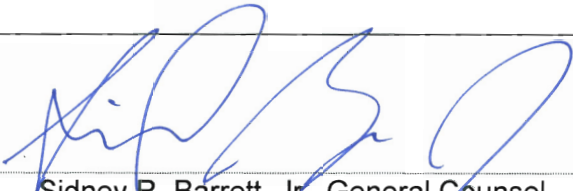

- Use confidential information only as needed to perform legitimate job responsibilities.
- Only access confidential information on a need to know basis.
- Not divulge, copy, release, sell, loan, review, alter, or destroy any confidential information except as authorized within the scope of my job responsibilities.
- Not misuse or carelessly handle confidential information.
- Safeguard any codes, keys, and passwords.
- Report activities by any other individual or entity that compromise the confidentiality and integrity of patient information.

I have received, read, understood, and agree to comply with this policy.

_____ Signature	_____ District Name or State Program	_____ Date
_____ Witness Signature	_____ Printed Name	_____ Date



**GEORGIA DEPARTMENT OF PUBLIC HEALTH  
POLICY # GC-09013  
CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION  
AND COMPLIANCE WITH HIPAA**

Approval:		30 August 2013
	Sidney R. Barrett, Jr., General Counsel	Date
		9/10/13
	James C. Howgate, Chief of Staff	Date

**TABLE OF CONTENTS**

**1.0 POLICY**

- 1.1 Authority
- 1.2 Definition of terms and acronyms

**2.0 APPLICABILITY AND RESPONSIBILITIES**

- 2.1 Applicability
- 2.2 Responsibilities

**3.0 GENERAL STANDARDS FOR HANDLING PROTECTED HEALTH INFORMATION**

- 3.1 Face to face discussions
- 3.2 Telephone calls
- 3.3 Visual access to PHI displayed on computer screens
- 3.4 Paper records and files
- 3.5 Outgoing mail (including inter-office or intra-office mail)
- 3.6 Facsimile communications
- 3.7 Emails

**4.0 THE "MINIMUM NECESSARY" RULE WHEN USING OR DISCLOSING PHI**

- 4.1 Necessary access or use
- 4.2 Minimum necessary disclosures
- 4.3 Situations in which the minimum necessary rule does not apply

**5.0 RESPONDING TO REQUESTS FOR DISCLOSURE OF PHI**

- 5.1 Requests for disclosure made by the patient
- 5.2 Requests for disclosure made by the patient's authorized representative
- 5.3 Requests for disclosure made by third parties with a written authorization from the patient
  - 5.3.1 Criteria for a valid authorization
  - 5.3.2 Authorization for disclosure of psychotherapy notes
  - 5.3.3 Invalid authorization
  - 5.3.4 Compound authorization
  - 5.3.5 Revocation of authorization
- 5.4 Requests for disclosure made by third parties without patient authorization

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	2 of 20		

5.5 Verification of identity prior to disclosure of PHI

- 5.5.1 Verifying a patient's identity
- 5.5.2 Verifying the identity and authority of the patient's personal representative
- 5.5.3 Verifying the identity and authority of a public official
- 5.5.4 Verifying the identity and authority of a law enforcement official

**6.0 OTHER REQUIREMENTS RELATING TO THE USE AND DISCLOSURE OF PHI**

- 6.1 De-Identification of PHI
  - 6.6.1 De-identification through statistician determination
  - 6.6.2 De-identification through removal of identifiers
  - 6.6.3 Re-identification
- 6.2 Limited data sets
- 6.3 "Business Associate" agreements

**7.0 REQUESTS FOR PHI CONTAINING RECORDS OF TREATMENT OR DIAGNOSIS OF MENTAL ILLNESS, HIV/AIDS, ALCOHOL OR DRUG DEPENDENCY, OR TREATMENT OF THE DEVELOPMENTALLY DISABLED**

**8.0 DOCUMENT RETENTION**

**9.0 TRAINING**

**10.0 PATIENT RIGHTS**

- 10.1 Right to notice of privacy practices
- 10.2 Right to request restriction of uses and disclosures of PHI
- 10.3 Right to request that communications be made in a confidential manner
- 10.4 Right of access to PHI

**11.0 COMPLAINT PROCEDURES**

**12.0 SANCTIONS AGAINST EMPLOYEES FOR VIOLATION OF POLICY**

- 12.1 Sanctions
- 12.2 Disclosures by whistleblowers
- 12.3 Refraining from intimidation or retaliation

**13.0 RESPONDING TO SUSPECTED BREACH OF PHI**

**14.0 RELATED FORMS AND POLICIES**

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	Revision #:	
<b>HIPAA</b>	<b>Page No</b>	3 of 20		

## 1.0 POLICY

The Department is committed to protecting the confidentiality of personal health information in accordance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all state and federal privacy laws. This policy sets forth the standards and procedures for Department employees to follow in protecting personal health information.

It is Department policy that 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.

This Policy does not list every possible situation in which the Department may lawfully disclose personal health information to third parties. Employees are directed to consult the DPH Privacy Officer if they believe it may be necessary to disclose an individual's personal health information without that individual's authorization.

### 1.1 AUTHORITY

45 C.F.R. Part 160: "General Administrative Requirements"

45 C.F.R, Part 162: "Administrative Requirements"

45 C.F.R, Part 164: "Security and Privacy"

### 1.2 DEFINITION OF TERMS AND ACRONYMS

1.2.1 **Administrative Safeguards:** Administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

1.2.2 **Breach:** The acquisition, access, use, loss, or disclosure of protected health information in circumstances where it might be accessed by unauthorized individuals or entities. If protected health information is acquired, accessed, used, lost, or disclosed in a manner not permitted under HIPAA or other privacy laws, then it shall be presumed to be a breach unless an investigation and risk assessment show that there is a low probability that the information was actually compromised.

1.2.3 **Business Associate:** An outside person or entity that performs or assists the Department in the performance of a function or activity involving the use or disclosure of individually identifiable health information.

1.2.4 **Covered Entity:** An entity that is subject to HIPAA because it is a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA.

1.2.5 **Covered Components:** Those Divisions, Programs, or Offices within DPH that have been designated as being subject to HIPAA because they perform the functions of a health plan, health care provider, or health care clearinghouse.

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	4 of 20		

- 1.2.6 **Designated Record Set:** A group of records that includes (1) the medical records and billing records about patients maintained by or for a covered health care provider; (2) records of the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) records used by or for the covered entity to make decisions about the patient. The term 'record' means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
- 1.2.7 **Disclosure:** The release or transfer of protected health information in any manner to a person or entity outside the Covered Component, including the act of allowing access to protected health information.
- 1.2.8 **Electronic Media:** Electronic storage media including memory storage components in computers and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, hard drive, or digital memory card; or transmission media used to exchange information already in electronic storage media. Examples of transmission media include the internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable/ transportable electronic storage media. Certain transmissions, such as facsimile messages, telephone conversations, or VOIP (voice over internet), are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.
- 1.2.9 **Electronic Protected Health Information:** Individually identifiable health information that is transmitted by electronic media or maintained in electronic media.
- 1.2.10 **Health Care Operations:** Any of the following activities of the covered entity to the extent that the activities are related to covered functions:
- 1.2.10.1 Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
  - 1.2.10.2 Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
  - 1.2.10.3 Underwriting and other activities relating to the creation, renewal, or replacement of a health insurance or health benefits contract, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
  - 1.2.10.4 Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
  - 1.2.10.5 Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
  - 1.2.10.6 Business management and general administrative activities including de-identifying protected health information, and creating a limited data set.

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	5 of 20		

- 1.2.11 **Health Care Provider:** A provider of services as defined in 42 U.S.C. 1395x(u), a provider of medical or health services as defined in 42 U.S.C. 1395x(s), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
- 1.2.12 **Health Information:** Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and which relates to the past, present or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present or future payment for the provision of health care to a patient.
- 1.2.13 **Health Oversight Agency:** An agency or authority of the United States, a territory, a political subdivision of a State or territory, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.
- 1.2.14 **Individually Identifiable Health Information:** Health information pertaining to an identifiable named patient, and which is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient, and that identifies the patient, or for which there is a reasonable basis to believe the information can be linked to the patient.
- 1.2.15 **Minor:** An unmarried person under the age of eighteen who has not been emancipated by order of the courts.
- 1.2.16 **Patient:** The person who is the subject of the protected health information.
- 1.2.17 **Protected Health Information (PHI):** Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
- 1.2.18 **Psychotherapy Notes:** Notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the patient's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
- 1.2.19 **Public Health Authority:** An agency or authority of the United States, a state, territory, a political subdivision of a state or territory, or an Indian tribe, or a person acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency, that is responsible for public health matters as part of its official mandate.

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	6 of 20		

- 1.2.20 **Security Incident:** The attempted or successful unauthorized access, use, disclosure, modification, loss, or destruction of health information, or interference with system operations in an information system that stores health information.
- 1.2.21 **Technical Safeguards:** The technology and the policy and procedures for its use that protect electronic protected health information and control its access.
- 1.2.22 **Unsecured Protected Health Information:** Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.

## 2.0 APPLICABILITY AND RESPONSIBILITES

**2.1 APPLICABILITY.** The Department has elected to designate itself as a “Hybrid Entity” for purposes of HIPAA compliance. This means that certain divisions, office, and programs within the Department must comply fully with HIPAA, and the rest are not subject to HIPAA. The following entities within the Department are hereby designated as Covered Components subject to HIPAA:

- 2.1.1 Within the Division of Health Protection: Public Health Laboratories; Pharmacy; Refugee Health; Volunteer Health Care Program; Epidemiology; Infectious Disease and Immunization.
- 2.1.2 Within the Division of Health Promotion: Maternal and Child Health; Health Promotion & Disease Prevention; WIC.
- 2.1.3 The Division of Information Technology.
- 2.1.4 District Health Directors and District Cadre Staff.
  - 2.1.4.1 The Department recognizes that County Boards of Health are separate legal entities employing their own public health employees, and that such County Boards of Health bear legal responsibility for their own HIPAA compliance. The District Health Director shall administer a legally sufficient HIPAA policy adopted by a County Board of Health with respect to its employees. If no such policy has been adopted by a County Board of Health, then the District Health Director shall administer this policy with respect to the county public health employees of that County.
- 2.1.5 DPH employees in Covered Components shall not disclose or allow access to PHI by DPH employees in other DPH divisions, offices, or programs except as specifically authorized by this policy or by the Privacy Officer. DPH employees in non-Covered DPH divisions, offices, or programs shall not have access to PHI except as authorized by the Privacy Officer.
- 2.1.6 Even though non-Covered DPH divisions, offices, and programs are not legally subject to HIPAA, it is expected that all DPH employees will familiarize themselves with the requirements of HIPAA and this policy, and will exercise their best efforts to protect the confidentiality of any individually identifiable health information which may come within their custody or control.

## 2.2 RESPONSIBILITES

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	7 of 20		

- 2.2.1 The Office of the General Counsel shall designate one of its members to serve as Privacy Officer for the Department, to be responsible for the development of the Department's policies and procedures for the protection of PHI and compliance with HIPAA, administrative safeguards, assistance with training materials, and providing legal advice as needed.
- 2.2.2 The Chief Information Officer shall designate a member of his or her staff to serve as Information Security Officer for the Department, to be responsible for the implementation of appropriate technical safeguards as required by HIPAA to ensure the integrity of all electronic PHI that the Department creates, maintains, receives, or transmits.
- 2.2.3 The Office of Human Resources is responsible for training of DPH employees in privacy compliance, for documenting such training for individual employees, and for applying appropriate sanctions against employees who violate privacy policies and procedures.
- 2.2.4 The District Health Director of each Health District shall designate a DPH employee to serve as District Privacy Officer for the Health District, to carry out the same responsibilities as the DPH Privacy Officer for that District.
- 2.2.5 The Security Incident Response Team shall respond to any suspected breach of PHI in accordance with the Personal Health Information Security Incident Response Protocol. The Team shall consist of the Privacy Officer and the Information Security Officer. If circumstances warrant, the Team may request the support of the Director of Communications, the Inspector General, and the District Privacy Officer.
- 2.2.6 Supervisory personnel in each Covered Component are responsible for ensuring compliance with this policy by DPH employees under their supervision.

### 3.0 GENERAL STANDARDS FOR HANDLING PROTECTED HEALTH INFORMATION

PHI should only be disclosed to people who have a legal right to receive it, whose identity has been verified, and whose authority to receive the PHI has been verified. In addition, care must be taken to prevent accidental disclosure or access to PHI by unauthorized persons.

**Note:** These standards apply even if the patient is deceased.

#### 3.1 Face to Face Discussions

Employees must take reasonable steps to protect the privacy of all face-to-face discussions of PHI, whether inside or outside of the office. When possible, employees should use enclosed offices or interview rooms for discussions involving PHI. If enclosed offices or rooms are not available, then employees should take reasonable precautions to ensure that their conversations are not overheard. In all cases, discussions of PHI should be limited to only that PHI which is necessary to conduct the business at hand.

#### 3.2 Telephone Calls

- 3.2.1 Before discussing PHI over the telephone with a patient, including providing test results or contacting the patient about appointments, employees must confirm the identity of the patient. This may be done by asking the patient to confirm his or her full name, date of birth, and the last four digits of their Social Security number.



<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	8 of 20		

- 3.2.2 Employees must honor any previously agreed upon requests by the patient to use alternate means of communication, such as alternate phone numbers, or limiting calls to certain hours.
- 3.2.3 Telephone calls should be made in private locations where possible. The employee should be aware of the surroundings and make sure that the conversation is not heard by nearby persons. The employee should also ask the patient to confirm that there is no one else on the line.
- 3.2.4 If the employee gets the patient's voicemail and decides to leave a message, then the message should only include the name and phone number of the person to be called back. Do not leave any other information, such as the name of the program from which the employee is calling or the fact that test results have been received, since that may compromise patient confidentiality if someone else retrieves the message.

### **3.3 Visual Access to PHI Displayed on Computer Screens**

- 3.3.1 Employees must ensure that PHI displayed on computer screens is adequately shielded from view by unauthorized persons. Polarized screens or other screen overlay devices that shield information on the computer screen should be used when possible.
- 3.3.2 Computer workstations must be locked when not in use, and PHI must be cleared from the screen when it is not being used.
- 3.3.3 Computers and other electronic storage devices containing PHI must be stored in a secured location at all times.

### **3.4 Paper Records and Files**

- 3.4.1 Employees must store files and documents containing PHI in secure filing cabinets, rooms, or storage systems. If lockable storage is not available, staff must take reasonable steps to ensure the safeguarding of documents containing PHI.
- 3.4.2 Papers containing PHI must be shredded before they are placed in the trash.
- 3.4.3 Documents containing PHI must be shielded from view by unauthorized persons, and should not be left unattended in open areas.

### **3.5 Outgoing Mail (Including Inter-office or Intra-office Mail)**

- 3.5.1 Documents or other medium containing PHI should be mailed in sealed envelopes or other secure container, properly addressed to the recipient, and the outer envelope should be clearly labeled "Confidential".
- 3.5.2 If PHI is stored on electronic media, then the media should be password protected before mailing.
- 3.5.3 The information sent should be the minimum necessary for the intended purpose.
- 3.5.4 All outgoing mail containing PHI should clearly display a return name and address on the outer envelope, so that misdirected mail can be returned to the sender.

### **3.6 Facsimile Communications**

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	9 of 20		

- 3.6.1 Covered Components must designate specific fax machines to send and receive documents containing PHI. The fax machines should be located in a non-public place and near to the intended recipients.
- 3.6.2 When receiving a fax containing PHI, employees should request a call from the sender prior to transmission, so that someone will be standing by to retrieve the document from the machine as soon as it received.
- 3.6.3 When sending a fax containing PHI, employees must contact the recipient to schedule transmission, confirm the fax number, and ensure that the fax will be retrieved by an authorized person after it is sent. Outgoing faxes containing PHI must have a cover page labeled "CONFIDENTIAL." After sending the fax, employees must confirm that delivery was made to the intended recipient by either contacting the recipient to confirm receipt or reviewing the fax transmission confirmation.
- 3.6.4 The information sent should be the minimum necessary for the intended purpose.
- 3.6.5 In the event that a fax is inadvertently sent to an unintended recipient, the recipient must be contacted immediately and asked to destroy the information. Misdirected faxes are considered a security incident and must be reported to the Privacy Officer.

### **3.7 Emails**

- 3.7.1 Emails should not contain PHI unless the PHI is in encrypted form. Where feasible, the PHI should be sent in a password-protected attachment instead of in the body of the email, with the password being sent in a separate email or communication which should also notify the recipient that the information has been emailed.
- 3.7.2 Emails containing PHI must be marked "CONFIDENTIAL" in the subject line, and should only be sent to persons who understand the Department's privacy policies and applicable privacy laws and regulations, and will not forward the email to unauthorized persons.
- 3.7.3 The information sent should be the minimum necessary for the intended purpose.
- 3.7.4 Employees should verify and review the recipient's email address prior to sending the email. In the event an email is inadvertently sent to the unintended recipient, the recipient must be contacted immediately and asked to delete the email and attachment. Misdirected emails are considered a security incident and must be reported to the Privacy Officer.

## **4.0 THE "MINIMUM NECESSARY" RULE WHEN USING OR DISCLOSING PHI**

Even when disclosure of PHI is appropriate, employees must ensure that only the minimum PHI necessary to accomplish the intended purpose will be used or disclosed.

### **4.1 Necessary Access and Use.**

Access and use should be restricted based on specific roles of persons working within a Covered Component. Each division, office, and program supervisor in a Covered Component must identify the persons or groups of persons who need access to PHI to carry out their job functions, identify the type of PHI to which each person or group needs access, as well as the conditions under which they need access, and make reasonable efforts to limit the access of its staff to only the information appropriate and necessary for their job requirements. Access to PHI should not be granted to any unit or program that does not need access to perform its job functions.

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	Revision #:	
<b>HIPAA</b>	<b>Page No</b>	10 of 20		

## 4.2 Minimum Necessary Disclosures:

Before disclosing PHI, staff must evaluate the purpose of the disclosure and limit the disclosure to the minimum necessary to satisfy the intent of the disclosure. Covered Components should identify routine and recurring disclosures and determine what information is reasonably necessary to fulfill the purpose of these requests so that the disclosure can be limited to the minimum necessary. In making this determination, Covered Components should evaluate whether the purpose of the disclosure can be fulfilled with de-identified information or a limited data set. Non-routine and non-recurring requests should be reviewed on an individual basis to ensure only the minimum necessary is disclosed for each of these requests.

### 4.2.1 Situations in which the minimum necessary requirement does not apply:

- 4.2.1.1 disclosures to or requests by a health care provider for treatment of the patient;
- 4.2.1.2 disclosures made to the patient or her authorized representative;
- 4.2.1.3 disclosures made pursuant to a valid authorization
- 4.2.1.4 disclosures made to the Secretary of the U. S. Department of Health & Human Services;
- 4.2.1.5 disclosures required by law; or
- 4.2.1.6 disclosures required for compliance with HIPAA regulations.

## 5.0 RESPONDING TO REQUESTS FOR DISCLOSURE OF PHI

### 5.1 Requests for Disclosure Made By the Patient

- 5.1.1 The Department shall disclose PHI to a patient when the patient requests access to their own PHI. However, there is one exception: a therapist's psychotherapy notes may not be disclosed to a patient without prior approval from the Privacy Officer.
- 5.1.2 The patient's identity shall be verified in accordance with Paragraph 5.5.1 before releasing PHI.

### 5.2 Requests for Disclosure Made By the Patient's Authorized Representative

- 5.2.1 The Department shall disclose PHI to a third party who is legally authorized to act as a representative of the patient with regard to health matters.
- 5.2.2 The scope of the representative's authority to act for the patient depends on his or her authority to make health care decisions for the patient. If the authority to act for a patient is limited to a particular health care decision, the person should be treated as the patient's representative only with respect to PHI relevant to that decision. Employees are encouraged to consult with the Privacy Officer if they have any doubt about the representative's authority.

Common situations involving a patient authorized representative include:

- 5.2.2.1 *Adult or Emancipated Minor*: If a person is authorized to act on behalf of an adult or emancipated minor in making health care decisions, then this person

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	11 of 20		

must be treated as a personal representative with respect to PHI related to such representation. Examples include persons acting pursuant to a health care power of attorney or general power of attorney, or a court appointed legal guardian.

5.2.2.2 *Deceased Patient:* Privacy rights under HIPAA continue for fifty years after the patient dies. An executor, administrator, or other person authorized by law to act on behalf of the deceased person's estate may be treated as personal representative with respect to the deceased's PHI.

5.2.2.3 *Minor Children:* If a parent, guardian, or other person acting in the place of a parent (*in loco parentis*) is authorized to act on behalf of a minor in making health care decisions, then this person may be treated as a personal representative with respect to PHI related to such representation. It may be necessary in some cases to require proof of a parent or other person's authority to have access to the child's PHI; for example, a divorced parent without authority to make health care decisions for the child should not have access to the child's PHI. In addition, the Department must *not* make disclosures to a parent or guardian if

5.2.2.3.1 the minor consented to care and the consent of the parent is not required under State or other applicable law (e.g., testing or treatment of venereal disease);

5.2.2.3.2 the minor obtained care at the direction of a court or a person appointed by the court; or

5.2.2.3.3 the parent or guardian agreed that the minor and the health care provider may have a confidential relationship.

5.2.2.4 *Married persons:* Employees are cautioned that a married person should *not* be given access to a spouse's PHI, unless that person presents proof of authorization in accordance with either this Paragraph or Paragraph 5.3.

5.2.3 The identity *and* authority of a third party seeking the PHI must be verified as specified in Paragraph 5.5 prior to disclosure of PHI to the third party. The proof needed to verify authority will vary depending on the nature of the authority. For example, a court-appointed guardian or the executor of a deceased person's estate will have an order of appointment from the probate court, and a person acting pursuant to a health care power of attorney will have a written power of attorney. Consult the Privacy Officer if you have any concerns about proof of authority.

5.2.4 The Department may refuse a request for PHI from a person acting as the patient's personal representative if it appears that the personal representative may have subjected the patient to violence, abuse, or neglect; if treating the person as a personal representative could endanger the patient; or if a licensed healthcare professional determines, in the exercise of professional judgment, that it is not in the best interest of the patient to treat the person as a personal representative.

### 5.3 Requests for Disclosure Made By Third Parties With a Written Authorization From the Patient

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	12 of 20		

A patient's PHI shall be disclosed to a third party pursuant to a valid written authorization signed by the patient. Patients should be encouraged to use the standard DPH Authorization For Release of PHI Form, but any authorization form that meets the requirements of Paragraph 5.3.1 should be honored. Upon request, the Privacy Officer shall review an authorization form to ensure that it is legally sufficient. The Department must retain a copy of all signed authorizations.

### 5.3.1 **Criteria for a Valid Authorization**

If an employee receives a request for disclosure of PHI from a third party with an Authorization Form signed by the patient attached, the form will be honored only if it contains all of the elements below in plain language:

- 5.3.1.1 A specific description of the information requested;
- 5.3.1.2 The name or other specific identification of the person(s), or class of persons, authorized to request the information;
- 5.3.1.3 The name or other specific identification of the person(s), or class of persons, to whom the Department may give the requested information;
- 5.3.1.4 A description of the purposes for which the information is requested;
- 5.3.1.5 An expiration date or an expiration event that relates to the patient or the purpose of the request;
- 5.3.1.6 Signature of the patient and date;
- 5.3.1.7 A statement adequate to place the patient on notice of his or her right to revoke the authorization in writing, a list of the exceptions to the right to revoke, and a description of how the individual may revoke the authorization;
- 5.3.1.8 A statement adequate to place the patient on notice of whether or not treatment, payment, enrollment or eligibility for benefits will be conditioned on whether the patient signs the authorization; and
- 5.3.1.9 A statement adequate to place the patient on notice of the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by HIPAA.

### 5.3.2 **Authorization for Disclosure of Psychotherapy Notes**

A separate specific authorization form must be obtained for the disclosure of psychotherapy notes that are included within a patient's medical records. The form must specifically request psychotherapy notes in addition to having all the elements listed in Paragraph 5.2.1. Consult with the Privacy Officer if there are any questions regarding the sufficiency of an authorization for the disclosure of psychotherapy notes received from a third party.

### 5.3.3 **Invalid Authorization**

An authorization will not be honored by the Department if it has any of the following defects: (i) the expiration date or event has passed; (ii) the Authorization Form has not been filled out completely; (iii) the authorization has been revoked; (iv) any information on

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	13 of 20		

the authorization is known to be false; (v) an authorization for psychotherapy notes is combined with a request for disclosure of information other than psychotherapy notes.

An invalid authorization should be returned to the person who submitted it, with an explanation of why the authorization cannot be honored. Consult with the Privacy Officer if you receive an authorization that may be invalid.

#### 5.3.4 **Compound Authorization**

An authorization for use or disclosure of PHI must be a separate document, and may not be combined with any other document from the patient to create a compound authorization, except as follows: (i) an authorization for the use or disclosure of PHI for a research study may be combined with the informed consent document that will be used in the research project; (ii) an authorization for the use or disclosure of psychotherapy notes may be combined with authorization for the use or disclosure of psychotherapy notes to other persons (e.g., a single authorization can be used for disclosure to multiple agencies or individuals); (iii) an authorization may be combined with authorization to other persons (e.g., a single authorization can be used for disclosure to multiple agencies or individuals).

#### 5.3.5 **Revocation of Authorization**

A patient may revoke his or her authorization in writing at any time. If the patient revokes an authorization, the Department cannot disclose information after the effective date of the revocation. A revocation should be maintained in the patient's file.

### 5.4 **Requests for Disclosure Made By Third Parties Without Patient Authorization**

Covered Components may disclose PHI to third parties without the written authorization of the patient only in certain limited circumstances. *All requests for disclosure without patient authorization must be sent to the Privacy Officer for review before any response is made.* The Privacy Officer may determine that disclosure of PHI without patient authorization is appropriate in the following situations:

- 5.4.1 To a healthcare provider covered by HIPAA for the purpose of treatment, payment, or healthcare operations;
- 5.4.2 Disclosures required by law;
- 5.4.3 Disclosures for public health activities to (i) Public Health Authorities that are authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including the reporting of disease, injury, vital events, and public health surveillance (e.g., the CDC); (ii) public health or other government authority legally authorized to receive reports of child abuse or neglect; or (iii) a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.
- 5.4.4 Disclosures about victims of abuse, neglect or domestic violence to a government authority authorized by law to receive such information under certain circumstances;
- 5.4.5 Disclosures for health oversight activities authorized by law (e.g., audits);
- 5.4.6 Disclosures for court proceedings, including search warrants, court orders, subpoenas, interrogatories, or requests for production of documents.

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	14 of 20		

**Note:** Any legal paper seeking PHI should be faxed, emailed, or hand-delivered to the Privacy Officer immediately upon receipt.

- 5.4.7 Disclosures for law enforcement purposes to a law enforcement official, if certain conditions are met;
  - 5.4.7.1 Disclosures about decedents to a coroner or medical examiner to identify a deceased person or determine cause of death, and to funeral directors;
  - 5.4.7.2 Disclosures for research purposes if approved in accordance with DPH Policy CO-12007 (Data Request Policy) and a DPH Data Use Agreement is signed;
  - 5.4.7.3 Disclosures to avert a serious threat to the health or safety of a person or the public;
  - 5.4.7.4 Disclosures for specialized government functions, including national security and intelligence activities;
  - 5.4.7.5 Disclosures to comply with laws relating to workers' compensations;
  - 5.4.7.6 Disclosures to persons involved in the patient's care and for notification of the patient's location, general condition, or death purposes. If the patient is present, he or she must be given the opportunity to agree or object to such disclosures.

**Note:** Disclosure of PHI is ordinarily *not* permitted in response to an Open Records Act request. Contact the Privacy Officer immediately if you receive an Open Records Act request for PHI.

## **5.5 Verification of Identity Prior to Disclosure of PHI**

Prior to making any permitted disclosure of PHI, Covered Components must verify the identity of the person requesting the PHI and the authority of such person or entity to receive such disclosure, if their identity or authority is not already known. Covered Components must also obtain any documentation, statements, or representations that are a condition of the disclosure from the person or entity making the request.

### **5.5.1 Verifying a Patient's Identity.**

The patient must provide their name, social security number, date of birth, address on file, and if available a copy of a government issued picture identification. Whenever practicable, requests should be in writing and signed by the patient. A copy of the request should be kept in the patient's file.

### **5.5.2 Verifying the Identity and Authority of the Patient's Personal Representative.**

Covered Components must verify the identity *and* authority of personal representatives requesting access to a patient's PHI. Covered Components must (i) verify the name and date of birth of the patient who is the subject of the request; (ii) obtain appropriate documentation supporting the request for access to the PHI, such as guardianship documents, custody orders, power of attorney, or Authorization Form; (iii) verify the requestor's name and obtain a copy of a government issued picture identification; (iv) confirm any limitations regarding the disclosure of information to the personal representative (v) once identity and authority has been confirmed, disclose only the minimum information necessary to fulfill the request.

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	Revision #:	
<b>HIPAA</b>	<b>Page No</b>	15 of 20		

### 5.5.3 Verifying the Identity and Authority of a Public Official.

Covered Components may rely on any of the following to verify identity of a public official:

- 5.5.3.1 If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- 5.5.3.2 If the request is in writing, the request is on the appropriate government letterhead; or
- 5.5.3.3 If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate governmental letterhead that the person is acting under the government's authority or other evidence or documentation, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

DPH may rely on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

- 5.5.3.4 A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or
- 5.5.3.5 If a request is made pursuant to legal process, then a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

### 5.5.4 Verifying the Identity and Authority of Law Enforcement Official.

Covered Components may disclose PHI to a law enforcement official for certain law enforcement purposes. The Covered Component should ask to see the law enforcement official's official identification and the subpoena, summons, request for records, civil or authorized investigative demand, or similar legal process by which the PHI is being requested, and then consult the Privacy Officer. A copy of this legal process should be kept in the patient's file.

## 6.0 OTHER REQUIREMENTS RELATING TO THE USE AND DISCLOSURE OF PHI

### 6.1 De-Identification of PHI

Disclosure of properly de-identified information is permitted by the HIPAA Privacy Rule. PHI is de-identified by removing certain individual identifiers to make it impossible to identify the health information as belonging to a particular patient. PHI is properly de-identified only if the information cannot be used alone or in combination with other information to identify a patient who is a subject of the information, **and** there is either a statistician determination pursuant to Paragraph 6.1.1 **or** removal of identifiers pursuant to Paragraph 6.1.2.

#### 6.1.1 De-Identification Through Statistician Determination.

Data is "de-identified" if a DPH employee with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data applies such principles and methods to the Data, and determines that such application



<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	16 of 20		

results in a very small risk that the de-identified data could be used, alone or in combination with other reasonably available information, to identify an individual whose de-identified PHI will be disclosed. Such a determination must be properly documented.

#### 6.1.2 De-identification Through Removal of Identifiers.

Data is “de-identified” through removal of the following identifiers of the individual or the individual’s relatives, household members, and employers: name, addresses (except for the State and the first three digits of the zip code, if the current total population of all zip codes with those three digits is more than 20,000), month and day of all dates directly related to an individual, all ages over 89 and all elements of dates indicative of such ages, telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers relating to Social Security, medical records, health plans, accounts, certificates, licenses, motor vehicles and license plates, drivers licenses, device and serial numbers, Internet Protocol (IP), and Universal Resource Locators (URLs).

#### 6.1.3 Re-identification.

Covered Components may assign a code or other means to allow de-identified information to be re-identified, provided that the code or other means is not derived from or related to information about the patient and cannot be translated to identify the patient, and the Department does not disclose the code or mechanism for re-identification.

### 6.2 Limited Data Sets

Covered Components may disclose a limited data set in accordance with DPH Policy CO-12007 (Data Request Policy) and pursuant to a DPH Data Use Agreement with the recipient of the limited data set. A limited data set may contain the following: town, city, state, zip code, date of birth, date of death, admission date, discharge date, ages, gender, race, ethnicity, marital status. However, the following identifiers of the individual or individual’s relatives, household members, employers must be removed: name, postal address information (other than town or city, State, and zip code), telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers relating to Social Security, medical records, health plans, accounts, certificates, licenses, motor vehicles and license plates, drivers licenses, device and serial numbers, Internet Protocol (IP), and Universal Resource Locators (URLs).

### 6.3 Business Associate Agreements

A business associate is a person or organization that, on behalf of the Department, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, or provides services to or for the Department which require access to PHI. All Covered Components must identify Business Associates, so that the appropriate contractual requirements are in place to govern the Business Associates’ use of PHI.

Before the Department discloses PHI to a business associate, the associate must sign the DPH Business Associate Agreement, or a contract to which the DPH Business Associate Agreement is attached. Any material breach or violation of the Business Associate Agreement must be reported to the Privacy Officer. If the Business Associate fails to cure the breach and end the violation, then its access to PHI must be cut off, and its contract with DPH must be terminated.

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	17 of 20		

## **7.0 REQUESTS FOR PHI CONTAINING RECORDS OF TREATMENT OR DIAGNOSIS OF MENTAL ILLNESS, HIV/AIDS, ALCOHOL OR DRUG DEPENDENCY, OR TREATMENT OF THE DEVELOPMENTALLY DISABLED**

**7.1** Employees are cautioned to consult with the Privacy Officer before releasing PHI which contains any reference to diagnosis or treatment of HIV/AIDS, drug or alcohol dependency or abuse, mental illness, or treatment of the developmentally disabled. Such records may be entitled to heightened legal protection in accordance with

7.1.1 O.C.G.A. § 37-3-166 (records of treatment of mental illness)

7.1.2 O.C.G.A. § 37-4-125 (records of treatment of the developmentally disabled)

7.1.3 O.C.G.A. § 37-7-166 (records of treatment for alcohol or drug dependency or abuse)

7.1.4 O.C.G.A. § 24-12-21 (records of testing, diagnosis, or treatment of HIV/AIDS).

## **8.0 DOCUMENT RETENTION**

All documents required by this Policy must be retained for six years from the date of creation or the date when it was last in effect, whichever is later, including its policies, standard forms and notices, and procedures in written or electronic form, all communications required to be in writing, and any action, activity or designation required to be documented. Although the HIPAA document retention period is six years, consult the Department's Record Retention Policy to ensure compliance with the Department's record retention schedule as well.

## **9.0 TRAINING**

The Office of Human Resources will develop online HIPAA training for use by all members of the workforce, and will collect and maintain a certificate of completion from each employee who completes the training. Training is required for all current employees, and for all new employees within 30 days of becoming employed, regardless of whether or not they work in a Covered Component. The content of the training will include key points of this Policy, and procedures for detecting, guarding against, and reporting malicious software. Periodic security updates will be distributed to the DPH workforce as changes are made to federal HIPAA regulations or this Policy and as needed.

## **10.0 PATIENT RIGHTS**

### **10.1 Right to Notice of Privacy Practices**

A copy of the current DPH Privacy Notice shall be given to each person receiving healthcare service from the Department. Covered Components must make a copy of the notice available to any person upon request, and for patients receiving treatment no later than the date of first service, or in an emergency treatment situation, as soon as reasonably practicable after the emergency. For patients receiving treatment, employees must make good faith efforts to obtain a written acknowledgement of receipt of the notice, and if unsuccessful, document good faith efforts to obtain the acknowledgement and the reasons it was not obtained. The written acknowledgement and documents showing efforts to obtain it must be maintained. The notice should be available at physical service delivery sites and posted in a clear and prominent location. The notice shall be posted on and made available through the Department's website.

### **10.2 Right to Request Restriction of Uses and Disclosures of PHI**

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	18 of 20		

10.2.1 Patients may request that the use and disclosure of their PHI be restricted to treatment, payment or health care operations, disclosures to persons involved in the patient's health care, or disclosures to notify family members or others about the patient's general condition, location or death. The Department is not required to honor such requests, but if it elects to do so, then the restriction must be documented and retained in the patient's file. Notwithstanding such a restriction, however, DPH may disclose the patient's PHI if it is needed for the purpose of treating the patient in the event of an emergency.

10.2.2 Patients may request that their PHI pertaining to a particular health care item or service *not* be disclosed to the patient's health plan, if that particular health care item or service was paid for without assistance from the patient's health plan. The Department must honor such a restriction. The restriction must be documented and retained in the patient's file.

### **10.3 Right to Request That Communications Be Made In a Confidential Manner**

Covered Components must accommodate reasonable requests by patients to receive communications of PHI by alternate means or at alternate locations or times. Employees must require that the request be in writing where possible. The patient must specify the requested alternate address or other method of contact, but need not give a reason for the request. The request must be documented and retained in the patient's file.

### **10.4 Right of Access to PHI**

10.4.1 A patient has a right of access to inspect and obtain a copy of his or her PHI in a designated record set, for as long as the PHI is maintained in a designated record set. All requests for access must be in writing and must be immediately forwarded to the Privacy Officer, so that the Department can act on the request within 30 days of receipt. Covered Components must document the designated record sets that are disclosed to patients and retain such documentation.

10.4.2 A patient's access to his or her PHI may be denied only in the following circumstances: psychotherapy notes may not be disclosed; the PHI was obtained from someone other than a healthcare provider and confidentiality was promised; or a licensed health care professional has determined that disclosure would endanger the life or safety of the patient or any other person. If access to any part of the patient's PHI is denied, then the patient shall be notified and given an opportunity to have the decision reviewed by a licensed health care professional who was not involved in the original decision.

10.4.3 The patient may request either paper or electronic copies of his or her PHI, and may be charged a reasonable fee to cover the cost of finding, copying, and providing the PHI.

### **10.5 Right to Request Amendment of PHI**

10.5.1 A patient has a right to have the Department amend PHI or a record about him or her in a designated record set, for as long as the PHI is maintained in a designated record set. All requests for amendments must be in writing and specify the reasons for the request, and shall be immediately forwarded to the Privacy Officer, so that the Department can act on the request within 60 days of receipt. The request must be documented and retained in the patient's file, along with any statement of disagreement submitted pursuant to Paragraph 10.5.2.

10.5.2 A patient's request for an amendment to his or her PHI may be denied only in the following circumstances: DPH did not create the PHI and the creator is available to act on the requested amendment; the information to be amended is not part of the designated record set; the PHI is

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	19 of 20		

accurate and complete; or the information is not lawfully subject to access by the patient. If any part of the patient's request is denied, then the patient shall be notified of the reasons, and given an opportunity to submit a statement of disagreement and to have the decision reviewed by a licensed health care professional who was not involved in the original decision.

## **10.6 Right to Request an Accounting of Disclosures of PHI**

A patient has a right to receive an accounting of disclosures of PHI made by the Department in the six years prior to the date on which the accounting is requested. All requests for accountings must be made in writing, and immediately forwarded to the Privacy Officer, so that the Department can act on the request within 30 days of receipt. The request should include the patient's name and specify the time period for which the accounting is being sought. The accounting must include disclosures of PHI for the time requested, including disclosures to or by Business Associates or for research purposes, date of the disclosure(s), name of the person or entity which received the PHI and, if known, the address, and a brief description of the information disclosed. A copy of the written request for an accounting and the accounting provided to the patient must be retained.

## **11.0 COMPLAINT PROCEDURES**

Complaints about the Department's compliance with its privacy policies and procedures and the HIPAA Rule shall be forwarded immediately to the Privacy Officer, along with as much information regarding the complaint as possible, including the complainant's name, contact information, date of incident, nature of complaint, to whom the PHI was improperly disclosed, any harmful effects that resulted, steps requested to limit the harm, and any additional comments. The Privacy Officer will investigate or oversee the investigation of the complaint, determine the appropriate response, and provide a written response to the complainant. Corrective action shall be taken as necessary, and appropriate sanctions will be imposed upon any employee who failed to comply with DPH privacy policies or HIPAA requirements. Documentation of complaints and their disposition will be retained by the Office of the General Counsel.

## **12.0 SANCTIONS AGAINST EMPLOYEES FOR VIOLATION OF POLICY**

### **12.1 Sanctions**

The Department shall apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Department or the requirements of the HIPAA regulations. Any violation of these policies or the HIPAA Privacy Rule will be reported to the employee's supervisor, the Privacy Officer, and the Office of Human Resources. The Office of Human Resources, will make a recommendation to the employee's supervisor about the appropriate sanction based on the nature of the violation. The type of sanction will vary depending on the severity of the violation, whether it was intentional or unintentional, and whether the employee engaged in a pattern of improper use or disclosure of PHI. Sanctions may include a warning, additional training, re-assignment of job functions, suspension, demotion, or other adverse actions up to and including termination of employment. The responsibility for training and managing the employee's job function will be considered. The employee will receive appropriate notice and opportunity to respond. Violations will be reviewed on a case by case basis, therefore sanctions may vary depending on the nature of violation. However, sanction will be applied with consistency to the extent possible. Sanctions will be documented and retained by the Office of Human Resources.

### **12.2 Disclosures by Whistleblowers**

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	GC-09013		
	<b>Effective Date:</b>	9/1/2013	<b>Revision #:</b>	
<b>HIPAA</b>	<b>Page No</b>	20 of 20		

An employee shall not be subject to sanctions for the inappropriate disclosure of PHI if the employee believes in good faith that the Department has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Department potentially endangers one or more patients, workers, or the public; and the disclosure is to (i) a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Department; or (ii) an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Department; or (iii) an attorney retained by or on behalf of the employee for the purpose of determining the legal options of the employee.

### **12.3 Refraining from Intimidation or Retaliation**

The Department may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any patient or other person for (i) filing of a complaint with the Secretary of the U.S. Department of Health and Human Services; (ii) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing conducted by the Secretary of the U.S. Department of Health and Human Services; or (iii) opposing any act or practice made unlawful by this subchapter, provided the patient or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule.

### **13.0 RESPONDING TO SUSPECTED BREACH OF PHI**

If any employee becomes aware of a possible acquisition, access, use, or disclosure of protected health information that is not permitted under HIPAA regulations and this policy, the employee must report the security incident within 24 hours to the Privacy Officer. All such incidents will be investigated by the Security Incident Response Team, and other staff as necessary, in accordance with the Personal Health Information Security Incident Response Protocol GC-00901E.

### **14.0 RELATED FORMS AND POLICIES**

DPH Form GC-00901A Business Associate Agreement

DPH Form GC-00901B Notice of Privacy Practices

DPH Form GC-00901C Authorization For Release of Protected Health Information

DPH Form GC-00901D Authorization For Release of Psychotherapy Notes

DPH Form GC-00901E Personal Health Information Security Incident Response Protocol

DPH Form GC-00901F Technological Safeguards for the Protection of Personal Health Information

DPH Data Use Agreement

DPH Data Request Policy No. CO-12007



## GEORGIA DEPARTMENT OF PUBLIC HEALTH PERSONAL HEALTH INFORMATION SECURITY INCIDENT RESPONSE PROTOCOL

This protocol sets out the procedures for responding to an actual or suspected personal health information security incident, and the responsibilities of persons tasked to respond to such incidents.

A **Security Incident** is an actual, suspected, or attempted loss or disclosure of individually identifiable personal health information within the custody or control of a DPH or County Board of Health employee. A Security Incident can take place in many different ways: the loss of a disk or laptop computer containing PHI, a malfunction or unauthorized attempt to enter into an information system on which PHI is stored, disclosure of PHI by email or telephone to the wrong person, an unauthorized modification or destruction of data, leaving papers with PHI in plain sight in a common area, etc.

A Security Incident shall be declared to be a **Breach** if protected health information was acquired, accessed, used, lost, or disclosed in a manner not permitted under HIPAA or other privacy laws, unless an investigation and risk assessment show that there is a low probability that the information was actually compromised.

The **Security Incident Response Team** consists of the DPH Privacy Officer and the DPH Information Security Officer. Depending on the circumstances of the incident, they may request the support of the Director of Communications or the Inspector General. If the Security Incident involves PHI within the custody of a county or District office, then the District Privacy Officer and District MIS Director will be on the Response Team.

### **Step One: Investigation.**

Any event that might possibly be a Security Incident shall be reported immediately to the Privacy Officer or Information Security Officer. The Security Incident Response Team shall immediately investigate the event, including personal interviews of any person who might have knowledge of the facts, and shall include the Director of Communications and Inspector General if necessary.

At the conclusion of the investigation, the Response Team shall decide whether there has been a Breach. The incident shall not be considered a Breach in the following circumstances:

- The acquisition, access, or use of the PHI was by a DPH employee or business associate in good faith and within the scope of their authority, and there was no further use or disclosure in violation of HIPAA;
- An inadvertent disclosure of PHI was made by a DPH employee or business associate authorized to access PHI to another DPH employee or business associate authorized to access PHI, and there was no further use or disclosure in violation of HIPAA;

- The PHI was disclosed to an unauthorized recipient, but there is a good faith belief that the recipient would not reasonably have been able to retain the PHI; or
- A risk assessment of the following factors by the Security Incident Response Team shows that there is a low probability that the PHI was compromised:
  - a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  - b. The unauthorized person who used the PHI or to whom the disclosure was made;
  - c. Whether the PHI was actually acquired or viewed; and
  - d. The extent to which the risk to the PHI has been mitigated.

### **Step Two: Response.**

Regardless of whether or not the Security Incident is deemed to be a Breach, the Security Incident Response Team shall develop and implement a plan to accomplish the following:

- Ensure that the conditions that made the incident possible are corrected so as to prevent future incidents. This may include recommendations for further training of employees, or changes to office technology, training, policy, or procedures.
- Identify individuals whose PHI was or may have been disclosed, and the persons or entities to whom PHI was or may have been disclosed.
- Mitigate any possible harm that may have resulted from the incident.
- Recommendations to the Office of Human Resources or District Health Director for disciplinary actions against persons responsible for the incident, if warranted.

### **Step Three: Notifications.**

If the Security Incident Response Team determines that there has been a Breach, then the Privacy Officer will advise on how to provide notice of Breach as required by law.

1. **To Affected Individuals:** Notice of a Breach shall be given to each affected individual. The Privacy Officer will prepare the notice in accordance with 45 CFR 164.404(c), and the program will be responsible to ensure that the notices are sent. The notice shall be written in plain language and contain the following:

- The date of breach, the date it was discovered, and a brief description of what happened;
- A description of the types of PHI that were involved (e.g., full name, Social Security number, date of birth, home address, account numbers, diagnoses, disability codes, etc.);
- Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
- A description of what DPH is doing to investigate the breach, mitigate harm to

- individuals, and protect against further breaches; and
- Contact information for individuals to ask questions or learn additional information, such as an email address, website, or mailing address.

The notice shall be sent by first-class mail to each individual's last known address; by email, if the individual has agreed to electronic notice; or to the next of kin or personal representative, if deceased. The Privacy Officer may approve another form of notice in accordance with 45 CFR 164.406 if the contact information for an individual or group of individuals is insufficient or out-of-date.

- 2. To Others:** If there are more than 500 affected individuals, then the Privacy Officer shall prepare a notice of the Breach for the Director of Communications to distribute to prominent media outlets serving Georgia no later than sixty days from discovery of the Breach. In addition, the Privacy Officer will provide notice to the Secretary of the U. S. Department of Health and Human Services as required by 45 CFR 164.408 contemporaneously with the notice to individuals, but no later than sixty days after discovery of the breach.



#### **Step Four: Documentation.**

At the conclusion of every investigation, the Privacy Officer shall ensure that a file is prepared and maintained to document the facts of the incident, the basis for the determination that there was or was not a Breach, the response, and proof that all notices required by law were made.





**GEORGIA DEPARTMENT OF PUBLIC HEALTH  
POLICY # IT-13002  
INFORMATION SECURITY PROGRAM POLICY**

Approval:		<i>2.25.14</i>
	Paul Ruth, Chief Information Officer	Date
		<i>2/28/14</i>
	James C. Howgate, Chief of Staff	Date

**1.0 PURPOSE**

The Department is committed to protecting the security of its information systems and data. This policy establishes the requirement for the Department to implement and maintain an internal information security infrastructure that safeguards the confidentiality, integrity, and availability of its information assets.

**1.1 AUTHORITY**

The Georgia Department of Public Health (DPH) Information Security Program Policy is published under the authority of DPH and in compliance with the following:

- 1.1.1 Georgia Technology Authority Enterprise Information Security Charter Policy PS-08-005.01
- 1.1.2 Official Code of Georgia Annotated (OCGA), Sections: 50-25-4(a)(21) and 50-25-4(a)(10)

**2.0 SCOPE**

This policy applies to the Georgia Department of Public Health.

**3.0 POLICY**

Department of Public Health will implement and maintain a formal information security program as a measure to protect the confidentiality, integrity, and availability of its information systems and data.

**4.0 DEFINITIONS**

- 4.1 **Information Security Infrastructure** - The interconnected elements (people, policies, processes, procedures and technology), that provide the framework to support an organization's security philosophy regarding their assets and effectively meeting their business objectives.

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	IT-13002		
	<b>Effective Date:</b>	7/1/2013	Revision #:	
<b>Information Security Program</b>	<b>Page No.</b>	2 of 3		

- 4.2 Confidentiality** - “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [44 U.S.C., Sec. 3542]. A loss of *confidentiality* is the unauthorized disclosure of information.
- 4.3 Integrity** - “Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., SEC. 3542]. A loss of *integrity* is the unauthorized modification or destruction of information.
- 4.4 Availability** - “Ensuring timely and reliable access to and use of information...” [44 U.S.C., SEC. 3542]. A loss of *availability* is the disruption of access to or use of information or an information system.
- 4.5 FISMA** - Federal Information Security Management Act requires each [federal] agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

## 5.0 RESPONSIBILITIES

- 5.1** The Chief Information Officer shall designate a member of his or her staff to serve as Information Security Officer, to have authority and responsibility for the implementation and management of the information security program.
- 5.2** The Information Security Officer shall develop, document, implement, and maintain the internal information security program to protect information assets.

## 6.0 PROCEDURES

- 6.1** The information security program shall:
- 6.1.1 Provide information security policies, standards, guidelines, processes, controls, and technology to protect information assets.
  - 6.1.2 Assess information risk to the confidentiality, integrity, and availability of information assets based upon the risk management framework established by the Federal Information Security Management Act (FISMA) of 2002.
  - 6.1.3 Ensure compliance with DPH, state, and federal requirements, such as but not limited to Health Insurance Portability and Accountability Act of 1996 (HIPAA).
  - 6.1.4 Meet DPH business objectives.

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b> <b>Information Security Program</b>	<b>Policy No.</b>	IT-13002		
	<b>Effective Date:</b>	7/1/2013	<b>Revision #:</b>	
	<b>Page No.</b>	3 of 3		


**7.0 REVISION HISTORY**

<b>REVISION #</b>	<b>REVISION DATE</b>	<b>REVISION COMMENTS</b>
0		Initial Issue





**GEORGIA DEPARTMENT OF PUBLIC HEALTH  
POLICY # HR-03403  
Work Away POLICY**

Approval:	 Kate Pfirman, Chief Financial Officer	10/14/12 Date
	 Dr. Brenda Fitzgerald, Commissioner	Date

**1.0 PURPOSE**

This policy contains guidelines for participation in the Work Away Initiative is a State of Georgia authorized work arrangement.

**1.1 AUTHORITY** – The Georgia Department of Public Health (DPH) Work Away Policy is published under the authority of DPH and in compliance with the following:

- 1.1.1 State Personnel Administration, formerly Georgia Merit System/Office of Planning and Budget Statewide Teleworking Policy – March 9, 2001
- 1.1.2 DPH Official Hours and Work Schedules Policy #HR03402
- 1.1.3 DPH Assignment of Duties Policy #HR03005
- 1.1.4 DPH Standards of Conduct and Ethics in Government Policy #HR03601

**2.0 SCOPE**

This policy applies to of the Department of Public Health.

**3.0 POLICY**

The policy of the Department of Public Health is to provide a State of Georgia authorized work arrangement that may be used as a recruitment and retention tool while providing positive impact on the environment, traffic gridlock and urban sprawl.

**3.1 ACCOUNTABILITY**

- 3.1.1 Work Away programs are voluntary work arrangements between an individual employee and his/her manager or supervisor.
- 3.1.2 The Work Away benefit is a privilege, not a universal benefit or right.

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	2 of 19		

3.1.3 The employee or manager/supervisor may terminate Work Away agreements at any time.

#### 4.0 DEFINITIONS

- 4.1 DPH – Georgia Department of Public Health
- 4.2 HR – DPH Division of Finance, Human Resources Section
- 4.3 FLSA – Fair Labor Standards Act
- 4.4 OSHA – Occupational Safety and Health Administration
- 4.5 **HR Work Away Coordinator** – the HR representative who oversees compliance with policies, procedures, agreements and guidelines and will report the results of Work Away programs in the Department to the Statewide Work Away Coordinator with the State Personnel Administration
- 4.6 **Unit Work Away Coordinator** – each Division Director or designee shall appoint a Work Away Coordinator to coordinate alternative schedules for his/her respective division.
- 4.7 **DPH Authorized Officials** – includes Section Directors and their designees
- 4.8 **Compressed Work Week (CWW)** – allows employees to work four 10-hour days in a week and therefore have one day off each week after 40 hours of work have been completed. *(For additional information pertaining specifically to Compressed Work Week, see section 6.2.1 of this policy which begins on page **Error! Bookmark not defined.**)*
- 4.9 **Alternate Work Week (AWW)** – allows employees to work four 9-hour days and one 8-hour day one week. The next week will have four 9-hour days and one day off. The day off must occur after an 80 hours of work have been completed. This schedule requires that for non-exempt employees the FLSA 7-day work period always begin in the middle of the 8-hour day. *(For additional information pertaining specifically to Alternate Work Week see section 6.2.1 of this policy which begins on page **Error! Bookmark not defined.**)*
- 4.10 **Teleworking** – allows employees to perform some or all of their work at a location other than the employee’s primary (usual and customary) work place. The alternate work place may include the employee’s home, a satellite office, or a teleworking center. *(For additional information pertaining specifically to Teleworking see section 6.2.2 of this policy which begins on page **Error! Bookmark not defined.**)*

#### 5.0 RESPONSIBILITIES



Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	3 of 19		

- 5.1** DPH Division of Finance, Human Resources Section (HR) is responsible for issuing and updating procedures to implement this policy.
- 5.2** The HR Work Away Coordinator is responsible for:
- 5.2.1 Overseeing compliance with policies, procedures, agreements and guidelines and will report the results of Work Away programs in the Department to the Statewide Work Away Coordinator with the State Personnel Administration.
  - 5.2.2 Working with the Unit Work Away Coordinators to ensure a successful Work Away program including collecting and compiling reports.
  - 5.2.3 All DPH employees who are authorized to participate in one or more of the Work Away programs must have a completed and signed a *Work Schedule Agreement Form* prior to starting the Work Away schedule. Completed forms should be kept on file with the manager/supervisor with a copy being forwarded to the HR Work Away Coordinator.
  - 5.2.4 The HR Work Away Coordinator will work with the Statewide Work Away Coordinator and Unit Coordinators to provide telework training programs.
- 5.3** The Unit Work Away Coordinator is responsible for:
- 5.3.1 Working with the HR Work Away Coordinator to ensure compliance with policies, procedures, agreements and guidelines.
  - 5.3.2 Providing Work Away data reports to the HR Work Away Coordinator as requested. Possibly be required to enter their unit's teleworking data into PeopleSoft each month. Collect the monthly random audit reports from manager/supervisors and submit to the HR Work Away coordinator.
  - 5.3.3 Verifying Teleworking training of the unit's employees and reporting on it as requested.
- 5.4** Responsibilities of Employees include:
- 5.4.1 Must be knowledgeable of the provisions of this policy.
  - 5.4.2 Employees who believe that one or more of the Work Away programs is appropriate for them and their position should discuss the potential Work Away program with their manager/supervisor.
  - 5.4.3 For participation in any Work Away program (i.e.: Teleworking, Compressed Work Week, or Alternate Work Week) in addition to any other forms that may be required, employees must complete, and submit to their manager/supervisor for approval, the following form:

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	4 of 19		

- *Work Schedule Agreement Form*

5.4.4 Employees who participate in Teleworking have these additional responsibilities:

5.4.4.1 In addition to the Work Schedule Agreement the following forms must also be completed and submitted to their manager/supervisor:

- Telework Agreement & Approval Form
- Telework Guidelines Form
- Telework Self-Assessment Form
- Telework Self-Certification of Work Space Form
- Property Removal Form - only required if the employee is to remove state property

5.4.4.2 Teleworkers and their manager/supervisor must complete the required training course prior to the employee beginning teleworking. (The Unit Work Away Coordinator is responsible for verifying training and ensuring that all required forms are on file.)

5.4.4.3 Establish a dedicated homework area/office consistent with the requirements of the Telework Guidelines and ensure that the site is safe and data and materials are secured. Passwords protect computers, jump drive, etc.

5.4.4.4 Establish work practices to ensure a successful teleworking experience. Submit to supervisor/manager completed time sheet showing times worked and accomplishments.

5.4.4.5 Report to department work sites for meetings, training, etc. as required by the manager/supervisor or other authorized official.

5.4.4.6 Determine any federal, state, or local tax implications regarding working at home and satisfy any personal obligations. DPH will not provide tax guidance or assume any additional tax liability. Employees are encouraged to consult with a qualified tax professional to discuss income tax implications.

5.4.4.7 Ensure that alternate worksite fully complies with all applicable local ordinances, zoning requirements and neighborhood association guidelines (i.e., community/sub-division covenants).

5.4.4.8 Comply with all provisions of this policy, the Telework Guidelines, the Telework Approval, and all other terms and conditions of employment.



Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	5 of 19		

5.4.5 Responsibilities of Manager/Supervisor include:

- 5.4.5.1 Must be knowledgeable of the provisions of this policy.
- 5.4.5.2 Review all documents submitted by the employee and objectively consider the employee's request within the provisions of this policy.
- 5.4.5.3 Determine if the Work Away arrangement is beneficial to the department and the employee. Approval should be based on Departmental, Division and organizational unit needs and coverage of official hours.
- 5.4.5.4 Ensure adequate staffing for the unit before approving the employee's Work Away request.
- 5.4.5.5 Review eligibility criteria of this policy listed in the Applicability section beginning on page **Error! Reference source not found.****Error! Bookmark not defined..**
- 5.4.5.6 If a Work Away program is determined appropriate, meet with the employee to sign the appropriate forms. For participation in any Work Away program (i.e.; Teleworking, Compressed Work Week, or Alternate Work Week); in addition to any other forms that may be required, the completed and signed *Work Schedule Agreement Form* must be forwarded to the HR Work Away Coordinator.
- 5.4.5.7 Retain a copy of all completed and signed forms for a period of one year after the Work Away arrangement ends. Provide the employee with a copy of all the completed and signed forms and ensure that the employee fully understands his/her responsibilities. Forward a copy of the approved form(s) to the HR Work Away Coordinator.
- 5.4.5.8 If the Work Away request is denied, provide written comments on the appropriate Agreement & Approval form(s) to the employee outlining the reason(s) for the decision. A denial of a Work Away request must be based on business-related reasons, documented in writing on the Agreement & Approval form(s), and made available to the employee. The explanation should outline any steps the employee can take to be eligible for reconsideration. This decision is final and is not appealable, grievable, or subject to review.



Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	6 of 19		

- 5.4.5.9 At the beginning of the Work Away arrangement, there is a 90-day probationary period.
- 5.4.5.9.1 During or immediately after the probationary period, a review should be conducted to determine if the Work Away program is the best work arrangement.
- 5.4.5.9.2 After the initial review, the Work Away Agreement is to be reviewed at least annually, when there is a major job change (e.g., promotion), when the Work Away employee or manager/supervisor change positions, or when any portion of the arrangement covered by the agreement changes. Appropriate modifications are to be made to the form(s), which must then be signed again by the employee and manager/supervisor.
- 5.4.5.10 Continue normal supervisory activities including feedback, performance evaluations; ensure that work is completed, etc.
- 5.4.5.11 Prepare an amendment to the employee's Performance Management Plan, specifically detailing responsibility areas and standards of performance pertaining to the terms of the appropriate Work form(s).
- 5.4.5.12 All Work Away schedules are to be reviewed and renewed or amended on an annual basis or as needed.
- 5.4.5.13 Additionally, for managers/supervisors who have Teleworking employees:
- 5.4.5.13.1 The following forms must also be completed:
- Telework Agreement & Approval Form
  - Telework Guidelines Form
  - Telework Self-Assessment Form
  - Telework Self-Certification of Work Space Form
  - Property Removal Form - only required if the employee is to remove state property
- 5.4.5.13.2 Completion of the required Manager Telework training course prior to their employees beginning teleworking. (The Unit Work Away Coordinator is responsible for verifying training.)
- 5.4.5.13.3 Ensure that performance can be adequately measured before authorizing teleworking and that

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	7 of 19		

sufficient work exists to enable the teleworking employee to work a productive day off-site.

5.4.5.13.4 Ensure adequate measures are in place to protect confidentiality and information security at the proposed alternate worksite;

5.4.5.13.5 Maintain an inventory of department-owned equipment in the employee's home or other alternate work place.

5.4.5.13.6 As necessary, perform site visit(s) to ensure safety compliance and adherence to the teleworking program requirements regarding the workspace and furnishing.

5.4.5.13.7 Report teleworking data to the Unit Work Away Coordinator or the designated official as requested.

5.4.6 Responsibilities of Authorized Officials include:

5.4.6.1 Must be knowledgeable of the provisions of this policy.

5.4.6.2 If required by program or requested by manager/supervisor:

5.4.6.2.1 Determine if the position/employee is suitable for the requested Work Away program.

5.4.6.2.2 Review employee submitted Agreement/Approval form(s);

5.4.6.2.3 If the request is denied, provide written comments on the Agreement & Approval form(s) outlining the reason(s) for the decision. Return the completed to the manager/supervisor, who will forward a copy to the employee.

## 6.0 PROCEDURES

6.1 All employees participating in a Work Away Program must meet the following criteria to be eligible unless a specific exception is granted by an authorized official:

6.1.1 Are full-time employees;

6.1.2 Have been employed with the department for at least six (6) months;

6.1.3 Have and maintain an annual leave balance of at least forty (40) hours;



<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	8 of 19		

- 6.1.4 Not currently involved in any type of disciplinary process, which would negatively impact the integrity of the Department of Public Health (DPH) Work Away Program. Examples include being on a work or attendance plan;
- 6.1.5 Have no record of misconduct in the last six (6) months that would cast doubt on the employee's ability to successfully work an alternative schedule. For example, an employee who disciplined for unauthorized absences from work may not be a suitable candidate for telework. Incidences of past misconduct or disciplinary action over six (6) months old may be considered in reviewing an employee's application if the action or misconduct causes employee's supervisor to be able to articulate a business-related reason that casts doubt on the employee's ability to successfully work an alternative schedule;
- 6.1.6 Have consistently met established productivity levels and received, at a minimum, overall ratings of 'Met Expectations' for both Responsibilities and Terms and Conditions of Employment on the most recent performance evaluation;
- 6.1.7 Additionally for employees to be also eligible to Telework they must:
- 6.1.7.1 Be in a position which is conducive to teleworking. i.e., a job that does not require access to material which cannot be moved from DPH offices and/or requires little or no special equipment to perform the job duties;
  - 6.1.7.2 Be self-motivated, responsible, and able to work independently;
    - 6.1.7.2.1 Be very familiar with requirements of the position,
  - 6.1.7.3 For an employee's position to be eligible to Telework they must have characteristics similar to the following may be considered for teleworking:
    - 6.1.7.3.1 Infrequent face-to-face communication requirements;
    - 6.1.7.3.2 Communication can be managed by telephone, cell phone, email, fax, etc.;
    - 6.1.7.3.3 Incumbent generally works alone handling or preparing information (e.g., researching, writing, preparing reports, developing procedures, creating planning documents, analyzing statistical data, etc.);
    - 6.1.7.3.4 Responsibilities have clearly defined results;

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	9 of 19		

- 6.1.7.3.5 Measurable work activities with objectives have identifiable time frames and check points;
- 6.1.7.3.6 Responsibilities are content versus process oriented;
- 6.1.7.3.7 Tasks which require concentration and/or large blocks of time when the employee works independently of others;
- 6.1.7.3.8 Alternative work place would not negatively impact service quality or organizational operations;
- 6.1.7.3.9 Work which can be performed without close supervision; and,

## 6.2 ALTERNATIVE SCHEDULES AND TELEWORKING

- 6.2.1 COMPRESSED WORK WEEK AND ALTERNATE WORK WEEK –a management options permitted by the department and are not employee rights. The duration of permission for Compressed and Alternate Work Week Schedules are entirely at the will and discretion of the department, which retains the prerogative to determine the time, place and manner of employment.
  - 6.2.1.1 An employee's participation in CWW or AWW is usually voluntary. The employee, manager/supervisor or other authorized official may terminate the program at any time; however, advanced notice should be given when feasible. Issues regarding approval are not appealable, grievable, or subject to review.
  - 6.2.1.2 The Work Schedule Agreement *Form* is to be reviewed and renewed or amended on an annual basis or upon any change in job responsibilities or the needs of the organizational unit or employee.
  - 6.2.1.3 Employee benefits (including leave and holidays) are not impacted by a Compressed or Alternate Work Week Schedule arrangement. Employees must follow established departmental policy relating to approval of leave.
  - 6.2.1.4 Compressed and Alternate Work Week schedules must be added to the employees Performance Plan. Employees will be evaluated in a manner similar to non-alternative scheduled employees.



<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	10 of 19		

- 6.2.2 TELEWORKING –a management option permitted by the department and is not an employee right. The duration of permission for Teleworking is entirely at the will and discretion of the department, which retains the prerogative to determine the time, place and manner of employment.
- 6.2.3 Employees may be allowed to telework when there are tangible benefits to the department and all expectations of the position are fully met. The job responsibilities of the position must be able to be satisfactorily performed away from the primary work place in order for teleworking to be considered.
- 6.2.4 Teleworkers must be mindful of the image presented during the teleworking day, and must not be involved in activities during the workday that will reflect negatively on the department. Examples include but are not limited to, working in the yard, shopping at the mall, being involved with other employment activities, etc.
- 6.2.5 An employee’s participation in teleworking is usually voluntary. The employee, manager/supervisor or other authorized official may terminate teleworking at any time; however, advanced notice should be given when feasible. Issues regarding approval for teleworking are not appealable, grievable, or subject to review.
- 6.2.6 The *Telework Agreement & Approval Form* is to be reviewed and renewed or amended on an annual basis or as needed.
- 6.2.7 Eligible Positions – Positions that have characteristics similar to the following may be considered for teleworking:
  - 6.2.7.1 Infrequent face-to-face communication requirements;
  - 6.2.7.2 Communication can be managed by telephone, cell phone, email, fax, etc.;
  - 6.2.7.3 Incumbent generally works alone handling or preparing information (e.g., researching, writing, preparing reports, developing procedures, creating planning documents, analyzing statistical data, etc.);
  - 6.2.7.4 Responsibilities have clearly defined results;
  - 6.2.7.5 Measurable work activities with objectives have identifiable time frames and check points;
  - 6.2.7.6 Responsibilities are content versus process oriented;
  - 6.2.7.7 Tasks which require concentration and/or large blocks of time when the employee works independently of others;

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	11 of 19		

6.2.7.8 Alternative work place would not negatively impact service quality or organizational operations;

6.2.7.9 Work which can be performed without close supervision; and,

6.2.7.10 Minimal requirement for special equipment.

#### 6.2.8 Personnel Considerations:

6.2.8.1 Teleworking must be added to the employees Performance Plan. Employees will be evaluated in a manner similar to non-teleworking employees.

6.2.8.2 Random audits will be conducted on a monthly basis to evaluate accountability and the success of the telework program including review of time sheets.

6.2.8.3 Employee benefits (including leave and holidays) are not impacted by a teleworking arrangement. Teleworking employees must follow established departmental policy relating to approval of leave.

6.2.8.4 Teleworking employees who work a set schedule should have an established work schedule with a beginning time and ending time, a scheduled meal period of at least thirty minutes, and identified break periods. Occasional teleworking employees are to discuss their work schedules with their manager/supervisor on an as needed basis.

#### 6.2.9 Emergency Situations

6.2.9.1 Although a variety of circumstances may affect individual situations, the principles governing administrative leave, dismissals and closings remain unchanged. The ability to conduct work (and the nature of any impediments), whether at home or at the office, determines when an employee may be excused from duty.

6.2.9.2 When situations arise that require closing of the office (i.e. inclement weather), teleworkers will be excused if regular office workers are excused. If Liberal Leave is declared, the teleworker can use leave or telework, if work is available.

6.2.9.3 When an emergency affects only the telework site (i.e. power outage, etc.), the teleworker is expected to report to the regular



<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	12 of 19		

office or request supervisory approval of annual leave, comp time, leave without pay, etc.

- 6.2.9.4 When a teleworker knows in advance of a situation that would preclude working at home, the employee must either come to the conventional office or request leave.

#### 6.2.10 Use of State-Owned Equipment

- 6.2.10.1 It may be permissible for the department to install telephone lines and other State-owned equipment in a teleworking employee's home. However, prior approval must be obtained from the DPH Chief Financial Officer through the HR Work Away Coordinator, and the use of such equipment and service must be for department business only and the department retains responsibility for the use, care and disposition of the State-owned property. If State-owned equipment is installed, the installation must consist of reversible procedures and retrievable personal property. The department may neither improve an employee's private property nor damage it in the process of installation.
- 6.2.10.2 All maintenance of State-owned equipment will be performed by an authorized DPH technician and may be conducted at DPH headquarters, or at a Division approved site.
- 6.2.10.3 Personally owned software may not be used on State-owned equipment.
- 6.2.10.4 Any and all software installed on State-owned equipment must be appropriately licensed.
- 6.2.10.5 The installation of State-owned equipment in a teleworking employee's home increases the legal complexity of the teleworking arrangement. Therefore, before a decision as to the installation of State-owned equipment or other service is made, managers should consult with the HR Work Away Coordinator and approval must be obtained by the DPH Chief Financial Officer.
- 6.2.10.6 ALL expenditures, (i.e., computers, printers, desks, chairs, DSL lines, internet lines, etc.), except general office supplies, must have prior approval of the DPH Chief Financial Officer or designee through the HR Work Away Coordinator.
- 6.2.10.7 Office supplies will be provided to the teleworker by DPH and should be obtained during the teleworker's in-office work period.

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	13 of 19		

DPH will not reimburse teleworkers for out-of-pocket expenses for supplies normally available in the office.

- 6.2.10.8 DPH may also give written permission for certain equipment to be checked out and used at the alternate work site. This equipment remains the property of the State and the department retains the responsibility for the inventory and maintenance of State-owned property following State laws and procedures. Employees are not authorized to use department issued equipment for personal use.
- 6.2.10.9 Issues relating to connectivity of State-owned equipment and security of information are subject to required standards of the Division of Information Technology. All systems MUST be password protected.
- 6.2.10.10 Transfer of State-owned equipment from the office to the telework site and back shall be the responsibility of the teleworker.
- 6.2.10.11 The employee's telework location is subject to department audits and security reviews as appropriate.
- 6.2.10.12 The teleworking employee's immediate supervisor shall maintain an inventory of State-owned equipment in employee's home.
- 6.2.10.13 The employee and employee's supervisor will complete and sign the Property Removal Form prior to the beginning of the work assignment.
- 6.2.11 Use of Employee-owned Equipment
  - 6.2.11.1 Teleworkers may use their own equipment (e.g. fax machine, printer, copier, etc.) provided that no cost is incurred by DPH. All expenses (e.g. maintenance, repair, insurance, etc.) shall be the responsibility of the teleworking employee.
  - 6.2.11.2 DPH does not assume liability for loss, damage or wear of employee-owned equipment.
  - 6.2.11.3 If a teleworker uses his/her personal computer, DPH files must be kept on separate disks or jump drives. The jump drives must be password protected.
  - 6.2.11.4 Software which is not appropriately owned by or licensed to DPH or the teleworking employee may not be run if DPH data



<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	14 of 19		

resides in the computer or if the computer accesses a DPH network.

6.2.11.5 All DPH information must be properly secured at the end of the business day. It will be incumbent upon the teleworking employee and his/her manager/supervisor to consult with Division of Information Technology to establish and implement an appropriate information security protocol.

6.2.11.6 In the event a piece of equipment (needed to accomplish work) is broken, needs repairs or otherwise becomes inoperable, the teleworker may be asked to report to the office until the equipment is fully functioning and usable.

#### 6.2.12 Fair Labor Standards Act (FLSA)

6.2.12.1 Teleworking employees must be accessible in some manner (e.g., telephone, cell phone, etc.) to their manager/supervisor, customers and coworkers during the agreed-upon work schedule regardless of the work location. Teleworkers may be asked to report to the primary work place on teleworking days should circumstances warrant.

6.2.12.2 FLSA non-exempt employees will be required to complete their regular time log at the end of each workweek and provide to their manager/supervisor to ensure compliance with the Fair Labor Standards Act. Part-time teleworking should be appropriately recorded on the document.

6.2.12.3 FLSA non-exempt employees must obtain prior approval from their manager/supervisor before performing overtime work. Failure to do so may result in the termination of the Telework Agreement and/or other appropriate action as necessary.

6.2.12.4 All teleworking employees should complete a time log.

6.2.12.5 Employees (FLSA exempt and non-exempt) may be required to complete a Telework Time Log to record work activity during the teleworking day. The form, if required by the manager/supervisor, should be submitted to the manager/supervisor on a weekly basis.

#### 6.2.13 Workers' Compensation

6.2.13.1 The teleworker's designated work area at his/her alternate work site will be considered an extension of DPH workspace. During the teleworker's designated work hours while he/she is

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	15 of 19		

performing work functions in the designated work area of the alternative work site, the teleworker will be covered by workers' compensation. It should be noted that attending to personal comfort needs is not considered performing official duties.

6.2.13.2 For purposes of workers' compensation coverage, the teleworker's "designated work hours" on his/her Work Schedule Agreement Form and "designated work area" shall be the area specified by employee on *Self-Certification of Work Space*. Employees and supervisors must take care to describe workspace and work hours on the appropriate forms to avoid confusion over workers' compensation coverage.

6.2.13.3 DPH assumes no liability for injuries occurring at the teleworker's alternate work site occurring outside the agreed-upon work hours or outside the agreed-upon designated work area. The teleworker must report on-the-job injuries to his/her supervisor as soon as possible after accident/injury occurs and submit supporting medical documentation of the accident/injury to his/her supervisor as soon as such documentation becomes available.

6.2.13.4 If necessary, teleworker shall permit the appropriate DPH representative to access the telework site to investigate an injury report.

#### 6.2.14 Worksite Safety and Liability

6.2.14.1 Any employee participating in telework is expected to perform his/her duties and responsibilities at the telework site at a proficiency level equal to or greater than when performed at the conventional office and work for the entire time period scheduled. Teleworkers must keep their alternative work site free from distractions and hazards and keep themselves free from obligations which would impair his/her ability to provide the same time and level of attention to the work product as when in the conventional office.

6.2.14.2 The teleworker's designated work area must meet OSHA safety rules for the workplace including: smoke detectors; working fire extinguisher; clear, unobstructed exits; removal of hazards that could cause falls; adequate electrical circuitry, and appropriate furniture.

6.2.14.3 As a condition of permission to telework, the employee must verify that the alternative work site used for telework purposes is safe and suitable for purposes of the employee's work. DPH



<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	<b>Revision #:</b>	1
<b>Work Away Policy</b>	<b>Page No.</b>	16 of 19		

may deny an employee the opportunity to telework if the alternate worksite is not conducive to productive work. DPH provides a Telework Self-Certification of Work Space Form as part of the application process to assist employee in the process.

- 6.2.14.4 DPH reserves the right to inspect the telework site to ensure safety compliance and adherence with the telework program requirements regarding space and furnishings.
- 6.2.14.5 DPH assumes no liability for any injuries to teleworker's family members, visitors or others in the employee's alternate work site. Teleworkers may not have business guests at the alternative worksite or any other location except DPH offices. Use of the telework site for work-related meetings is prohibited. Teleworkers may be required to come into the office or utilize teleconferencing if a work-related meeting becomes necessary.
- 6.2.14.6 DPH shall not be responsible for any loss or damage to: the teleworker's real property, including any structures attached thereto; any personal property owned by the teleworker, or any of the teleworker's family members; or property of others in the care, custody or control of the teleworker or any of the teleworker's family members.
- 6.2.14.7 The teleworker shall be responsible for contacting his/her insurance agent and tax consultant and consulting local ordinance, restrictive covenants and applicable neighborhood association guidelines for information regarding home workplaces.
- 6.2.14.8 Individual tax implications, auto and homeowners insurance, and incidental residential utility costs are the responsibility of the teleworker.

6.2.15 Dependent Care

- 6.2.15.1 DPH offers teleworking opportunities to employees with the understanding that it is the responsibility of the employee to ensure that a proper work environment is maintained. The employee and his/her family must understand that the designated work area is a space set aside for the employee to work. Family responsibilities should not interfere with work time.
- 6.2.15.2 Teleworking is not a substitute for childcare or dependent care. The teleworker shall continue to make arrangements for child

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	17 of 19		

or dependent care to the same extent as if the teleworker was working in a conventional office.

#### 6.2.16 Telework Confidentiality Information Security

6.2.16.1 Security of confidential information is of primary concern and importance. Teleworkers, like all State employees, are expected to adhere to all applicable laws, rules, regulations, policies and procedures regarding information security. All information assets (equipment, software, and confidential information) used within the Telework Program are subject to these security policies.

6.2.16.2 Divisions allowing employees to access records subject to the Privacy Act from an alternate work site must maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. Security and confidentiality protection measures shall be discussed by employee and his/her supervisor and included in the Telework Agreement & Approval Form.

6.2.16.3 To help ensure confidentiality and information security, Teleworker shall:

6.2.16.3.1 Be responsible for maintaining confidentiality and security at the alternative workplace, as the teleworker would at the primary workplace. The teleworker must protect the security and integrity of data, information, paper files, and access to agency computer systems. DPH's internet and technology use policies apply to teleworking as they would in the primary work place. Ensure that confidential information is not disclosed to unauthorized people.

6.2.16.3.2 Ensure that the software used for teleworking is virus inspected and each PC used by the teleworker has virus protection software installed.

6.2.16.3.3 Return all material (paper documents, diskettes, etc) containing confidential information to the office work site for proper handling or disposal (e.g., Certified Destruction), if necessary, or shred through a personal shredder.

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	<b>Revision #:</b>	1
<b>Work Away Policy</b>	<b>Page No.</b>	18 of 19		

- 6.2.16.3.4 Adhere to copyright law by not copying or sharing any State-owned software utilized by teleworkers.
- 6.2.16.3.5 Safeguard confidential departmental information maintained in files, in computers, on diskettes, etc. Where the hard disk of an alternate workplace computer is inoperable, arrangements must be made to remove sensitive information from the hard disk prior to having the computer serviced. This procedure must be followed regardless of whether the computer is owned by the employee or DPH.
- 6.2.16.3.6 Immediately notify Information Technology and your Division Work Away Coordinator of any suspected or actual security violation. The division coordinator will notify the HR Work Away Coordinator.
- 6.2.16.3.7 All external drives, jump drives and computers are to be password protected.
- 6.2.16.3.8 Understand that adherence to the above is an essential requirement of the Telework Program. Failure to comply with the provisions may be cause for canceling participation in the Telework Program and/or possible adverse action.
- 6.2.16.3.9 Minimal requirement for special equipment.

## 7.0 REVISION HISTORY

REVISION #	REVISION DATE	REVISION COMMENTS
0	November 7, 2011	Initial Issue
1	July 23, 2012	Annual review and update. Reformat to new template



Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	HR-03403		
	<b>Effective Date:</b>	11/07/11	Revision #:	1
<b>Work Away Policy</b>	<b>Page No.</b>	19 of 19		

## 8.0 RELATED FORMS

*HR03402A – Work Schedule Agreement Form*

*HR03403A – Telework Agreement & Approval Form*

*HR03403B – Telework Guidelines Form*

*HR03403C – Telework Self-Assessment Form*

*HR03403D – Telework Self-Certification of Work Space Form*

*HR03403E – Telework Time Log Form*

*HR03403F – Governor's Executive Orders*

*AM01001A – Property Removal Form*



**GEORGIA DEPARTMENT OF PUBLIC HEALTH  
POLICY # CO-12007  
DATA REQUEST POLICY**

Approval:		11/5/13
	James Howgate, Chief of Staff	Date

**1.0 PURPOSE**

This policy contains guidelines for the disclosure and protection of data maintained by the Georgia Department of Public Health to researchers undertaking research for legitimate scientific public health purposes.

This policy shall not apply to data requests from a news organization or other member of the media. All such requests shall be promptly referred to the Director of Communications.

This policy shall not apply to data requests from a governmental entity. All such requests shall be promptly referred to the Privacy Officer in the Office of the General Counsel.

**1.1 AUTHORITY** – The Georgia Department of Public Health Data Request Policy is published under the authority of DPH and in compliance with the following:

- 1.1.1 Health Insurance Portability and Accountability Act of 1996.
- 1.1.2 45 CFR Subparts 160, 162, and 164
- 1.1.3 O.C.G.A. §§ 31-22-9.1, 21-12-24

**2.0 SCOPE**

This policy applies to every person employed by DPH.

**3.0 DEFINITION OF TERMS AND ACRONYMS**

**3.1 AIDS Information** – Information which discloses that a person has been diagnosed as having AIDS, has been or is being treated for AIDS, has been determined to be infected with HIV, has submitted to an HIV test, has had a positive or negative result from an HIV test, has sought and received counseling regarding AIDS, or has been determined to be a person at risk of being infected with HIV or AIDS, and which permits the identification of that person.

**3.2 DPH** – Georgia Department of Public Health

**3.3 IRB** – Institutional Review Board

**3.4 PHI** - Protected Health Information

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	CO-12007		
	<b>Effective Date:</b>	8/15/13	Revision #:	
Data Request	<b>Page No.</b>	2 of 6		

PHI means any information, whether oral, written, electronic, visual, pictorial, physical, or any other form, that relates to an individual's past, present, or future physical or mental health status, condition, treatment, service, products purchased, or provision of care, and which (a) reveals the identity of the individual whose health care is the subject of the information, or (b) where there is a reasonable basis to believe such information could be utilized (either alone or with other information that is, or should reasonably be known to be, available to predictable recipients of such information) to reveal the identity of that individual. For example, if a health record contains sufficient information to identify an individual to whom it relates because it provides information which specifically narrows the class of individuals in an aggregate setting, such record may be considered identifiable in its existing form, and thus PHI.

- 3.5 **Data request** means an inquiry from any person or entity for data or information collected by or housed within the Department that requires compilation or aggregation by DPH staff.
- 3.6 **Disclosure** means the release, transfer, provision of, access to, or divulging in any other manner of information outside DPH.
- 3.7 **Legitimate scientific purpose** means a population-based activity or individual effort conducted pursuant to guidelines accepted by the research community.
- 3.8 **Public Health** means the physical, mental and social well-being of the community.
- 3.9 **Public Health Authority** means an agency or authority of the United States, a state, territory, a political subdivision of a state or territory or an Indian tribe or a person or entity acting under a grant of authority from or contract with such public agency that is responsible for public health matters as part of its official mandate.

#### 4.0 PERMITTED DISCLOSURES AND RESTRICTIONS ON DISCLOSURES

- 4.1 **Permitted Disclosures:** DPH may disclose data for legitimate scientific research purposes relating to public health. DPH shall have the sole discretion to determine what constitutes a legitimate scientific purpose relating to public health.
- 4.2 **Restrictions on Disclosures:** Data maintained by DPH shall not be disclosed for commercial purposes.
- 4.3 **AIDS Information:** AIDS Information shall not be disclosed except in de-identified form, according to the protocol set forth in Paragraph 8.2.2.

#### 5.0 RESPONSIBILITIES

- 5.1 DPH Governance Council is responsible for issuing and updating procedures to implement this policy.



<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	CO-12007		
	<b>Effective Date:</b>	8/15/13	Revision #:	
Data Request	<b>Page No.</b>	3 of 6		

**5.2** Each Division and Office is responsible for ensuring that all data requests are processed in compliance with this policy.

## **6.0 PROCEDURES**

**6.1 Submission of Data Requests.** All data requests shall be submitted through the Georgia Public Health Information Portal (PHIP).

**6.2 Functions of the Data Coordinator.** The Data Coordinator is responsible for overseeing the process from receipt of the data request to release of the data to the requestor. Specific responsibilities include:

6.2.1 Reviewing each data request and identifying the information being requested;

6.2.2 Promptly referring all media requests to the Director of Communications;

6.2.3 Coordinating with the Privacy and Open Records Officer to determine whether the request is valid and the information can be released under applicable law;

6.2.4 Coordinating with the DPH IRB to determine if the data request will be used for research that requires IRB review and approval;

6.2.5 Routing request to appropriate program contact person or Data Analyst for completion, and following-up as necessary to ensure accurate and timely completion of the request;

6.2.6 Communicating with the requestor as necessary; and

6.2.7 Maintaining accurate records of the requests in the PHIP database.

**6.3 Functions of the Data Analyst.** The Data Analyst is responsible for compiling the data requested. Specific responsibilities of the Data Analyst include:

6.3.1 Timely completion of the data request;

6.3.2 Performing quality checks to ensure accuracy of the compiled data set.

**6.4 IRB Review.** When necessary, research for which data is requested shall be reviewed by the researcher's Institution's IRB and DPH IRB for compliance with all applicable laws and regulations.

**6.5 Data Use Agreement.** Prior to receiving any data, the requestor must sign a Data Sharing Agreement which is attached to this policy, along with the Terms and Conditions of the Data Sharing Agreement.

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	CO-12007		
	<b>Effective Date:</b>	8/15/13	Revision #:	
Data Request	<b>Page No.</b>	4 of 6		

## 7.0 USE OF DATA PROVIDED BY DPH IN PUBLICATIONS AND PRESENTATION

**7.1 Credit and Authorship.** DPH shall be referenced as the source of the data in all publications or presentations for which the requested data will be used, or, if appropriate, DPH and the researcher will agree upon the terms of authorship. DPH may request to review any draft publication or presentation and reject any such draft if the findings are inconsistent with the original purpose of the request, or with DPH's mission.

## 8.0 DATA REQUESTS INVOLVING PHI

**8.1 Disclosure of PHI.** If the data to be provided constitutes or includes individually identifiable PHI, then only the minimum amount of PHI necessary to accomplish the purposes of the research may be used or disclosed. The DPH Privacy Officer should be notified of any Data Use Agreement that calls for individually identifiable personal health information to be disclosed, along with the names of the individuals whose PHI will be disclosed, and the disclosure must be noted in the individual's designated record set.

**8.2** The requirements of one of the following four paragraphs must be satisfied in connection with every Data Use Agreement that calls for the disclosure of PHI:

**8.2.1. Institutional Review Board Approval.** The Recipient provides documentation that an Institutional Review Board meeting the standards cited in 45 CFR 164.512(i)(1)(i)(A) has approved the waiver of the individuals' authorization for the release of their PHI, or has approved an alternation to such an authorization. This documentation must include the signature of the IRB chair; the name and contact information for the IRB and the date on which the alteration or waiver was approved; a description of the specific PHI needed for the research project; an affirmative statement that the IRB has reviewed and approved the request for waiver or alternation in accordance with the normal or expedited review procedures and other requirements of the Common Rule; and an affirmative statement that the IRB has determined that the waiver or alteration of the individuals' authorization satisfies the following criteria:

8.2.1.1. The use of the PHI involves no more than a minimal risk to the privacy of the individuals, based on an adequate plan to protect against the improper use and disclosure of identifiers, an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research (unless there is a health, legal, or research justification for retaining the identifiers), and adequate written assurances that the PHI will not be reused or disclosed except for lawful purposes;

8.2.1.2. The research could not practicably be conducted without the waiver or alteration; and

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	CO-12007		
	<b>Effective Date:</b>	8/15/13	Revision #:	
Data Request	<b>Page No.</b>	5 of 6		

8.2.1.3. The research could not practicably be conducted without the access to and use of the PHI.

8.2.2. **De-Identification of Data.** The Data is de-identified before disclosure to the Recipient using one of the following two methods:

8.2.2.1. A DPH employee with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data applies such principles and methods to the Data, and documents that such application results in a very small risk that the de-identified data could be used, alone or in combination with other reasonably available information, to identify an individual whose de-identified PHI will be disclosed to the Recipient; or

8.2.2.2. The Data is scrubbed of the following identifiers of the individual or the individual's relatives, household members, and employers: name, addresses (except for the State and the first three digits of the zip code, if the current total population of all zip codes with those three digits is more than 20,000), month and day of all dates directly related to an individual, all ages over 89 and all elements of dates indicative of such ages, telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers relating to Social Security, medical records, health plans, accounts, certificates, licenses, motor vehicles and license plates, drivers licenses, device and serial numbers, Internet Protocol (IP), and Universal Resource Locators (URLs); and there is no actual knowledge that the information can be used alone or in combination with other information to identify the individual.

8.2.3. **Limited Data Sets.** The Data is provided to the Recipient in the form of a limited data set, from which the following identifiers of the individual or individual's relatives, household members, employers have been scrubbed: name, postal address information (other than town or city, State, and zip code), telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers relating to Social Security, medical records, health plans, accounts, certificates, licenses, motor vehicles and license plates, drivers licenses, device and serial numbers, Internet Protocol (IP), and Universal Resource Locators (URLs).

8.2.4. **Research on Deceased Individuals.** The Data pertains only to deceased individuals, and the Recipient affirms in writing that access to the Data is sought solely for the purpose of conducting research on the PHI of

<b>Department of Public Health POLICY AND PROCEDURES</b>	<b>Policy No.</b>	CO-12007		
	<b>Effective Date:</b>	8/15/13	Revision #:	
Data Request	<b>Page No.</b>	6 of 6		

deceased individuals and that the PHI is necessary for its research purposes. If DPH does not already have information positively identifying the PHI as belonging to deceased individuals, then the Recipient must provide documentation of the death of the individuals whose PHI is sought.

## 9.0 PROCESSING FEES:

9.1 All data requests are subject to a processing fee, representing a reasonable estimate of the Department's cost to prepare and transmit the Data. The fee is non-refundable regardless of the outcome of the search and must be paid before the request is filled. The fee schedule is as follows:

9.1.1 Individual data requests: \$200 base fee + \$25 per variable used, per data year

9.1.2 Ongoing data requests / Subscriptions: \$200 base fee + \$25 per variable used for the initial request and \$200 for each renewal of the same data request

9.2 Exemptions from processing fees may be granted for the following:

9.2.1 Requests from academic faculty, unless the data will be used for a project funded from sources external to DPH

9.2.2 Requests from undergraduate or graduate students, unless the data will be used for a project funded from sources external to DPH

9.2.3 Requests from DPH employees, unless the data will be used for a project funded from sources external to DPH

9.2.4 Internal data exchanges between DPH programs/divisions

## 10.0 REVISION HISTORY

REVISION #	REVISION DATE	REVISION COMMENTS
0		Initial Issue
1		

## 11.0 RELATED FORMS

CO-12007A - *Terms and Conditions for Data Sharing Agreements*

CO-12007B - *Data Sharing Agreement*





GEORGIA DEPARTMENT OF PUBLIC HEALTH  
POLICY # CO-12009  
DATA STANDARDS POLICY AND PROCEDURES

Approval:		10/1/13
	James C. Howgate, Chief of Staff	Date

**1.0 PURPOSE**

To reduce redundancy in data management; to assure data integration is possible; to leverage DPH information assets for purpose of better decision-making.

**1.1 AUTHORITY** – The Georgia Department of Public Health (DPH) Data Analysis and Reporting Policy and Procedures is published under the authority of DPH and in compliance with the following:

1.1.1 DPH Governance Council

**2.0 SCOPE**

This policy applies to all data collected and managed in the department that will be used for DPH analysis and reporting.

**3.0 POLICY**

The policy of the Department of Public Health is that all data collected and managed in the department that will be used for DPH analysis and reporting shall adhere to the DPH Data Quality Principles and with the DPH Data Property Standards.

3.1. The policy of DPH shall be guided by the following principles:

- 3.1.1. A variable shall have one and only one name.
- 3.1.2. A variable shall have one and only one definition.
- 3.1.3. A variable shall be stored in one and only one data type.
- 3.1.4. A variable shall have one and only one field length.
- 3.1.5. A variable shall be stored in one and only one unit of measurement.
- 3.1.6. A variable shall be stored in one and only one level of measurement.
- 3.1.7. A variable shall represent or store only those values specified in its definition.
- 3.1.8. Data objects shall have one and only one source.

<b>Department of Public Health</b> <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	CO-12009		
	<b>Effective Date:</b>	10/1/2013	Revision #:	
<b>DATA STANDARDS</b>	<b>Page No.</b>	2 of 9		

- 3.1.9. No duplicate sources of data objects shall exist.
- 3.1.10. No duplicate records shall exist in data objects.
- 3.1.11. All data domains, data objects and variables shall be free of data anomalies.
- 3.1.12. Unknown, missing and inapplicable values shall have respectively unique representations.
- 3.1.13. Unknown, missing and inapplicable values in all data domains shall have consistent representations as defined in 3.1.12.
- 3.1.14. All data dictionaries shall define the following data properties for each variable: Variable Name, Variable Storage Name, Variable Definition, Variable Data Type, Unit of Measurement, Level of Measurement, Unit of Analysis, Level of Analysis, Variable Field Length, Variable Precision, Variable Time Stamp, and Variable Associated Standards. If a data property is not applicable for a variable, "n/a" shall be noted.

#### **4.0. ACCOUNTABILITY**

- 4.1 DPH application business owners collecting and managing data.

#### **6.0 DEFINITIONS**

- 6.1 Appendix A shows definitions of each Data Quality Principle

#### **7.0 RESPONSIBILITIES**

- 7.1 The DPH Model Team shall ensure compliance to this policy (or procedure).
  - 7.1.1 DPH application business owners collecting and managing data.

#### **8.0 PROCEDURES**

Consult and adhere to the Standard Data Properties as found in Appendix B.

Applies to:

- New system development
- Existing system modifications
- Active acquisition of existing data sources destined for the DPH data warehouse.

Department of Public Health <b>POLICY AND PROCEDURES</b>	<b>Policy No.</b>	CO-12009		
	<b>Effective Date:</b>	10/1/2013	Revision #:	
<b>DATA STANDARDS</b>	<b>Page No.</b>	3 of 9		

## 9.0 REVISION HISTORY

REVISION #	REVISION DATE	REVISION COMMENTS
0	10/01/2013	Initial Issue
1		

## 10.0 RELATED FORMS

- Appendix A: Data Quality Principles – Definitions
- Appendix B: Standard Data Properties



## Data Quality Principles – Definitions

These principles serve as a reference for all data quality management.

1. **A variable shall have one and only one name.** Example: the data item “sex” is named “sex” as opposed to “gender.” Or, if a database collects information about “permits,” then that construct shall not also be referred to as a “certification.”
2. **A variable shall have one and only one definition.** Example: The definition of white race is:  
A person having origins in any of the original peoples of Europe, the Middle East or North Africa (OMB directive-15, 1997).
3. **A variable shall be stored as one and only one data type.** For example, string data such as ICD codes (cause of death codes with values such as A018, 001.1) should not be stored as a numeric field.
4. **A variable shall have one and only one field length.** Example: collection of street address should allow for 60 characters, not less.
5. **A variable shall be stored in one and only one unit of measurement.** Example: Birthweight is stored in grams, but not pounds and ounces.
6. **A variable shall be stored in one and only one level of measurement.** Example: a *nominal* variable such as “race” shall not be stored as *interval* data.
7. **A variable shall be represented by or stored as only those values specified in its definition.** Example: if 1=yes and 0=no, there should be no other values (e.g., 9, 8, z, abc) found in that field.
8. **Data objects shall have one and only one source.** For example: official Georgia Birth statistics will come from the Office of Health Indicators for Planning, Georgia Department of Public Health.
9. **No duplicate sources of data objects (storage or collection) shall exist.** Example: A central data repository for analytic health information shall contain each data domain (such as vital records, notifiable diseases, immunizations).
10. **No duplicate records shall exist in data objects.** Example: One and only one record for each birth in the birth data domain.
11. **All data domains, data objects and variables shall be free of data anomalies.** All data assets will be examined for invalid values and such values will be processed such that their values are in a known state.
12. **Unknown, missing and inapplicable values shall be represented by one known value.** Example: 99 (unknown), nulls, blanks, or out of range values all set to = -1.
13. **Unknown, missing and invalid values in all data domains shall have consistent representations as defined in 12.**
14. **All data dictionaries shall define the following data properties for each variable.**



The properties are in the following table:

Variable Name(s)	Name of the data item used for storage and if applicable, presentation. Storage names begin with a domain identifier (e.g. Birth), followed by an owner (e.g. Mother), followed by the variable name (e.g. birth.mother.education_level). Presentation name (or label) is used to present data, such as "Mother's education level."
Definition and Variable Associated Standards	A statement containing the reason to collect or use the variable and external standards that apply to the variable.
Valid Values	Acceptable values for the variable being defined (e.g. mother's age range = 10-55 years inclusive.).
Data Type	The characteristic of a variable that determines what kind of data it can hold. For example, data types include Byte, Boolean, Integer, Long Integer, Currency, Decimal, String, Double, and Date.
Field Length	The number of numerical places or characters for a specific field.
Unit of Measurement	(a) refers to the system of measurement: English or metric; (b) the specific unit, within a measurement system, at which measurements for a variable are made such as grams.
Level of Measurement	(1) Nominal: One data element is identified as disparate from another but no direction is implied. Categorical properties or labels; such as the variable race represented by White, Black or African-American, American Indian or Alaska Native, Asian, and Native Hawaiian or Other Pacific Islander; or Male/Female. Appropriate descriptive statistics are the mode (most commonly occurring value) and frequency counts; (2) Ordinal: Variables can be ranked to show one value is more or less than another value; however the difference cannot be calculated, such as 'high/medium/low.'" Objects are ordered by some nominal category irrespective of magnitude, and irrespective to the distance between ordered levels; such as variable representing the level of agreement with a statement represented by disagree, somewhat agree, agree, disagree. Appropriate statistics are the mode, frequency, median (middle value), and percentiles. (3) Interval: Variables have an established identical distance between them on a scale; however they do not have a true zero, such as grams, inches, days. Ordering of objects is respective to a nominal category, the distance between objects respective to the nominal category, and without respect to the magnitude of the nominal category such as the number of hours a client waited for service measured in hours represented by 1, 2, 3, 4 etc. Appropriate statistics are the mean (average), median, mode, standard deviation (square root of the variance), range (maximum value – minimum value) and percentiles. (4) Ratio: Have a true zero. Objects are ordered respective to a nominal category, where the distance between objects is known, and each objects measurement is respective to a known zero value such as annual income measured in dollars represented by 20,051, 55,987, 42,042, etc.
Unit of Analysis	The unit of measurement assigned to a variable for analysis.
Level of Analysis	The level of measurement assigned to a variable for analysis.
Derivation	For calculated fields, the variables used and method to derive the calculated variable.
Time Stamp of Standard	The date on which the variable definition was defined or revised.



## Standard Data Properties

## PERSON (Age, Race, Ethnicity, Sex)

Property	Value
Presentation Name(s)	<b>AGE</b>
Definition	Elapsed time since birth. Age in years at the time of this event. Age is reported as age at last birthday - that is, age in completed years, and calculated by subtracting date of delivery from the reference date, with the reference date being the date of the examination, interview, or other contact with an individual (NCHS).
Valid Values	0 - 44,194 days. 0 – 120 years. (44,194 translates into 120 years); -1=unknown. Four (4) years = (365 x 4) + 1.
Data Type	Long Integer
Field Length	5
Unit of Measurement	Day
Level of Measurement	Interval
Unit of Analysis	Day
Level of Analysis	Interval
Derivation	EVENT_DATE – DOB = AGE IN DAYS. CONVERT TO YEARS FOR PRESENTATION.
Time Stamp of Standard	3/27/2002.

Property	Value
Presentation Name(s)	<b>RACE</b>
Definition	White = a person having origins in any of the original peoples of Europe, the Middle East or North Africa; Black or African-American = A person having origins in any of the black racial groups of Africa; Asian=A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand and Vietnam; American Indian/Alaska Native=A person having origins in any of the original peoples of North and South America (including Central American), and who maintains tribal affiliation or community attachment; Native Hawaiian or Other Pacific Islander=A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands. Multiracial = 2 or more of these races (OMB-15, 1997).
Valid Values	1=White, 2=Black or African American, 3=Asian, 4=American Indian/Alaska Native, 5=Native Hawaiian / Pacific Islander, 6=Multiracial; -1=unknown.
Data Type	Integer
Field Length	2
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Time Stamp of Standard	6/12/2000.

Property	Value
Presentation Name(s)	<b>ETHNICITY</b>
Definition	Ethnicity, currently limited to asking whether the person is "Hispanic or Latino" (A person of Mexican, Puerto Rican, Cuban, South or Central American, or other Spanish culture or origin, regardless of race) (OMB-15, 1997).
Valid Values	1=Hispanic or Latino, 0=No; -1=unknown.
Data Type	Integer
Field Length	2
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Derivation	Practice in vital records for pre-03 version of certificates: Derived from Origin values 1-5 inclusive.
Time Stamp of Standard	3/16/2000 per U.S. OMB Directive 15, 1997.

Property	Value
Presentation Name(s)	<b>SEX</b>
Definition	Biological sex
Categorical Attributes	Male / Female
Valid Values	1=Male, 2=Female, -1=unknown.
Data Type	Integer
Field Length	2
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Time Stamp of Standard	5/4/2000.

**"Place" requires COLLECTION of 4 data items: Street, City, State, and Zip such that geocoding can assign a latitude/longitude.**

Specifications for collection of each follow:

Property	Value
Presentation Name(s)	<b>STREET ADDRESS</b>
Definition	Geographic street address of event owner, event, or facility.
Valid Values	Street number followed by street name, followed by street direction (e.g. NW), followed by Apartment identifier, followed by room identifier. Storage of street names will follow standard abbreviations such as RD, BLVD, LN, ST. (See <a href="http://www.gis.co.clay.mn.us/usps.htm">http://www.gis.co.clay.mn.us/usps.htm</a> ) -1 = Unknown.
Data Type	String
Field Length	60
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Derivation	Self-report.
Time Stamp of Standard	3/16/2000 2.10.2004 – no need to proclaim "0"=Out of state. 6.10.13 – updated spec to be 60 characters instead of 40.



Property	Value
Presentation Name(s)	<b>CITY NAME</b>
Definition	For use in collection of city names: Geographic city or town or parish or Census Designated Place (CDP) or village where the event occurred or event owner lived.
Valid Values	USPS City Names; -1 = unknown, 0=non-Georgia resident, _UNIN = resident/event in an unincorporated place (not in a city limit).
Data Type	STRING
Field Length	27
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Derivation	A collection item. City is Derived from latitude/longitude via a Geocoding process where applicable, and stored as a city code.
Time Stamp of Standard	3/16/2000. 1/23/07

Property	Value
Presentation Name(s)	<b>ZIPCODE</b>
Definition	Geographic zipcode+4 where the event owner lived or where event occurred, using USPS standard zipcodes.
Valid Values	USPS zipcodes; -1 = unknown. 0=non-Georgia zip.
Data Type	String
Field Length	9
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Derivation	Derived via geocoding where applicable. Originals stored as *_original.
Time Stamp of Standard	3/16/2000

Property	Value
Presentation Name(s)	<b>STATE</b>
Definition	Geographic state of residence or event.
Valid Values	USPS postal abbreviations.
Data Type	String
Field Length	2
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Derivation	Self-report
Time Stamp of Standard	3/16/2000

### Place **STORAGE** standards

Property	Value
Presentation Name(s)	<b>LATITUDE</b>
Definition	Latitude of event or residence.
Categorical Attributes	N/A
Valid Values	- - - 0 = non-georgia.
Data Type	Floating point.
Field Length	Float
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless

Level of Analysis	Nominal
Derivation	Derived from geocoding process, using Street, City, State, Zip.
Time Stamp of Standard	3/16/2000. See issue 177.
Access	<input type="checkbox"/> Public Use <input checked="" type="checkbox"/> Datamart Variable
<b>Property</b>	<b>Value</b>
Presentation Name(s)	<b>LONGITUDE</b>
Definition	Longitude of event or residence.
Categorical Attributes	N/A
Valid Values	- - 0 = non-Georgia.
Data Type	Floating point.
Field Length	Float.
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Derivation	Derived from geocoding process, using Street, City, State, Zip.
Time Stamp of Standard	3/16/2000. See issue 177.
Access	<input type="checkbox"/> Public Use <input checked="" type="checkbox"/> Datamart Variable

<b>Property</b>	<b>Value</b>
Presentation Name(s)	<b>COUNTY</b>
Definition	Geographic county of event or residence.
Valid Values	Two digit state FIPS code 00-99 followed by three digit FIPS county code 000-999; range 13001-13321; 0=Non-Georgia county, -1 = unknown.
Data Type	String
Field Length	5
Unit of Measurement	Unitless
Level of Measurement	Nominal
Unit of Analysis	Unitless
Level of Analysis	Nominal
Derivation	Derived from geocoding where applicable. Note encapsulated rules for event county in specific instances.
Time Stamp of Standard	3/16/2000. 0 for non-ga 10.21.2003.

## TIME

<b>Property</b>	<b>Value</b>
Presentation Name(s)	<b>DATE</b>
Definition	Date of an event.
Valid Values	Months (mm)=01-12 / Days (dd)=01-31 / Year (ccyy)=18yy, 19yy, or 20yy; 12/31/9999=unknown.
Data Type	Date
Field Length	10
Unit of Measurement	Day
Level of Measurement	Interval
Unit of Analysis	Day
Level of Analysis	Interval
Time Stamp of Standard	3/27/2002.