City of Pittsburgh
Operating Policies

Policy: HIPAA Privacy Policies and Procedures	Original Date: 1/2005 Revised Date: 3/22/2010

PURPOSE: To establish internal policies and procedures to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) as it pertains to the protected health information of City employees.

POLICY STATEMENT: The City of Pittsburgh Group Health Plan has established and maintains a methodology for consistent organization-wide development, training, review, approval, assessment and updates of policies and procedures as they pertain to HIPPA regulations.

All of the City of Pittsburgh Group Health Plan HIPAA Privacy Policies and Procedures are included in the pages that follow.

Disclaimer: No statements in this policy are intended or set forth as contractual commitments or obligations of the City to any individual employee or group of employees, or to establish an exception to the employment-at-will doctrine beyond that specified in the Civil Service Statutes and Rules or pertinent collective bargaining agreement. If there are differences between the various collective bargaining agreements and this policy, the pertinent collective bargaining agreement takes precedence.

CITY OF PITTSBURGH

THE CITY OF PITTSBURGH GROUP HEALTH PLAN
(THE "PLAN")

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT OF 1996 ("HIPAA")

POLICIES AND PROCEDURES

Compliance Dates:
April 14, 2003 (for HIPAA Privacy Requirements)
April 20, 2005 (for HIPAA Security Requirements)

Effective Revision Date – November 30, 2009

Note: copies of these Policies and Procedures must be retained for the later of six (6) years from the date they became effective or were last in use.

CITY OF PITTSBURGH

THE CITY OF PITTSBURGH GROUP HEALTH PLAN
(THE "PLAN")

Policies and Procedures Manual

Table of Contents

Sec.	Topic	Citation
1.9	Safeguards	45 CFR §164.530(c)
2.0	**Authorization**	
2.1	Authorization for Uses and Disclosures of PHI	45 CFR §164.508, §164.532(a)
3.0	**Business Associates**	
3.1	Business Associates and Contracts	45 CFR §164.502(e), §164.504(e), §164.520, §164.524(b)(2), §164.528(b), §164.530(f), §164.532 (d) and 164.308(b)(1)
4.0	**Disclosure of PHI to Plan Sponsor**	
4.1	Disclosure of PHI to Plan Sponsor	45 CFR §164.504(f)
4.2	Granting Levels of Access to PHI	45 CFR §164.504, §164.530
5.0	**Individual Rights**	
5.1	Individual's Right to Access PHI	45 CFR §164.524
5.2	Individual Request to Amend PHI	45 CFR §164.526
5.3	Individual's Rights to Request Privacy Protection for PHI	45 CFR §164.522
5.4	Complaint Process	45 CFR §164.530(a)(1)(ii), §164.530(d)
5.5	Notice of Privacy Practices	45 CFR §164.520

Sec.	Topic	Citation
6.0	**Minimum Necessary**	
6.1	Minimum Use of PHI	45 CFR §164.502(b) and §164.514(d)
7.0	**Training**	
7.1	Training Workforce Regarding Protection of Health Information	45 CFR, §164.530(b)
8.0	**Uses and Disclosures**	
8.1	Uses and Disclosures of PHI	45 CFR §164.502(a) and (g), §164.506, §164.510, §164.512
8.2	Accounting (Logging) of Disclosures of Member PHI	45 CFR §164.528
9.0	**Administrative Safeguards**	
9.1	Security Management Process	45 CFR §164.308(a)(1)(i)
	9.1.1 Risk Analysis	45 CFR §164.308(a)(1)(ii)(A)
	9.1.2 Risk Management	45 CFR §164.308(a)(1)(ii)(B)
	9.1.3 Sanctions	45 CFR §164.308(a)(1)(ii)(C)
	9.1.4 Information System Activity Review	45 CFR §164.308(a)(1)(ii)(D) and 45 CFR §164.312(b) – (c)(2)
9.2	Assigned Security Responsibility	45 CFR §164.308(a)(2)

Sec.	Topic	Citation
9.3	Workforce Security	45 CFR §164.308(a)(3)(i)
	9.3.1 Authorization and/or Supervision (A)	45 CFR §164.308(a)(3)(ii)(A)
	9.3.2 Workforce Clearance Procedure (A)	45 CFR §164.308(a)(3)(ii)(B)
	9.3.3 Termination Procedures (A)	45 CFR §164.308(a)(3)(ii)(C)
9.4	Information Access Management	45 CFR §164.308(a)(4)(i)
	9.4.1 Access Authorization (A)	45 CFR §164.308(a)(4)(ii)(B)
	9.4.2 Access Establishment and Modification (A)	45 CFR §164.308(a)(4)(ii)(C)
9.5	Security Awareness and Training	45 CFR §164.308(a)(5)(i)
	9.5.1 Security Reminders (A)	45 CFR §164.308(a)(5)(ii)(A)
	9.5.2 Protection from Malicious Software (A)	45 CFR §164.308(a)(5)(ii)(B)
	9.5.3 Log-in Monitoring (A)	45 CFR §164.308(a)(5)(ii)(C)
	9.5.4 Password Management (A)	45 CFR §164.308(a)(5)(ii)(D)
9.6	Security Incident Procedures	45 CFR §164.308(a)(6)(i)
	9.6.1 Response and Reporting	45 CFR §164.308(a)(6)(ii)
9.7	Contingency Plan	45 CFR §164.308(a)(7)(i)(A) – (E)
	9.7.1 Data Backup Plan	45 CFR §164.308(a)(7)(ii)(A)
	9.7.2 Disaster Recovery Plan	45 CFR §164.308(a)(7)(ii)(B)
	9.7.3 Emergency Mode Operation Plan	45 CFR §164.308(a)(7)(ii)(C)
	9.7.4 Testing and Revision Procedures (A)	45 CFR §164.308(a)(7)(ii)(D)
	9.7.5 Applications and Data Criticality Analysis (A)	45 CFR §164.308(a)(7)(ii)(E)

Sec.	Topic	Citation
9.8	Periodic Evaluation	45 CFR §164.308(a)(8)
10.0	**Physical Safeguards**	
10.1	Facility Access Controls	45 CFR §164.310(a)(1)
	10.1.1 Contingency Operations (A)	45 CFR §164.310(a)(2)(i)
	10.1.2 Facility Security Plan (A)	45 CFR §164.310(a)(2)(ii)
	10.1.3 Access Control and Validation (A)	45 CFR §164.310(a)(2)(iii)
	10.1.4 Maintenance Records (A)	45 CFR §164.310(a)(2)(iv)
10.2	Workstation Use	45 CFR §164.310(b)
10.3	Workstation Security	45 CFR §164.310(c)
10.4	Device and Media Controls	45 CFR §164.310(d)(1) - (2)(iv)
	10.4.1 Disposal	45 CFR §164.310(d)(2)(i)
	10.4.2 Media Re-Use	45 CFR §164.310(d)(2)(ii)
	10.4.3 Accountability (A)	45 CFR §164.310(d)(2)(iii)
	10.4.4 Data Backup and Storage (A)	45 CFR §164.310(d)(2)(iv)

Sec.	Topic	Citation
11.0	**Technical Safeguards**	
11.1	Access Control	45 CFR §164.312(a)(1)
	11.1.1 Unique User Identification	45 CFR §164.312(a)(2)(i)
	11.1.2 Emergency Access Procedure	45 CFR §164.312(a)(2)(ii)
	11.1.3 Automatic Logoff (A)	45 CFR §164.312(a)(2)(iii)
	11.1.4 Encryption and Decryption (A)	45 CFR §164.312(a)(2)(iv)
11.2	Audit Controls	45 CFR §164.312(b)
11.3	Integrity	45 CFR §164.312(c)(1)
	11.3.1 Mechanism to Authenticate ePHI (A)	45 CFR §164.312(c)(2)
11.4	Person or Entity Authentication	45 CFR §164.312(d)
11.5	Transmission Security	45 CFR §164.312(e)(1)
	11.4.1 Integrity Controls (A)	45 CFR §164.312(e)(2)(i)
	11.4.2 Encryption (A)	45 CFR §164.312(e)(2)(ii)
12.0	**Breach of Unsecured PHI**	
12.1	Notification to Individuals	45 CFR §164.404
	Notification to the Media	45 CFR §164.406
	Notification to HHS	45 CFR §164.408
	Administrative Requirements	45 CFR §164.503

Introduction to the Plan's HIPAA Policies and Procedures

In compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the City of Pittsburgh Group Health Plan (referred to in this Manual as the "Plan") has established internal practices on how to handle employees' Protected Health Information (PHI) and to safeguard the Confidentiality, Integrity and Availability of Individuals' electronic PHI (ePHI).

PHI is Individually Identifiable Health Information that is transmitted or maintained in any form or medium by a HIPAA Covered Entity, such as the Plan. (ePHI is PHI which is transmitted or maintained in electronic form.) Examples of materials containing PHI could include eligibility, enrollment and disenrollment information provided to insurers that provide coverage for Plan participants; benefit design analyses; premium rate calculations; reinsurance quotes; materials relating to the provision of legal, actuarial, and auditing services to the Plan; and general data analysis used in the long-term management and planning for the Plan.

Importantly, PHI excludes employment records, other records held by the City of Pittsburgh in its role as employer (the "City" or the "plan sponsor"), and information relating to non-HIPAA covered benefits, such as disability, life, and workers' compensation insurance. This can include information that is obtained and/or held in relation to FMLA and ADA requests, sick leave requests, and benefits plan enrollment information.

HIPAA Background

Through HIPAA, the federal government has defined and standardized practices and procedures that describe how certain PHI may be used and disclosed and how Individuals can access their PHI and ensure that their rights are protected. This federal law:

- Defines the groups that review and handle PHI;
- Protects Individually Identifiable Health Information;
- Provides Individuals with the right to access their own PHI;
- Requires Authorization to Use and Disclose PHI; and
- Ensures participants receive adequate notice of their privacy rights.

Policy and Procedure Highlights

The objective of the practices outlined in this document is to define how the Plans may handle and share PHI and how the City has established reasonable and appropriate safeguards to ensure the Confidentiality, Integrity and Availability of our Individuals' ePHI and to protect this information from reasonably anticipated improper or unauthorized access, alternation, deletion and transmission. A few highlights include:

- Administrative Procedures, including how to verify an Individual's identity and how to audit the privacy Standards;
- Authorizations, including when one is needed in using and disclosing PHI;
- Business Associates, including how to identify them and the contract language needed for the sharing of PHI by and with Business Associates;
- Individual Rights, including the right to request PHI and restrict some of its Disclosures;
- Administrative Safeguards, including an overview of our Security management process, Security Incident procedures, access management, and periodic evaluation policy;
- Physical Safeguards, including our Facility access controls, Workstation Use and Security policies, and device and media controls;
- Technical Safeguards, including technology-based access and audit controls, Authentication methods, and data transmission and Integrity controls; and
- Training and awareness for employees who handle PHI and ePHI.

It is important for you to read this document carefully and understand your role in handling and protecting PHI and ePHI under HIPAA. There is a Glossary of Terms and Definitions in Appendix A of this Manual. Those Terms and Definitions are capitalized within this Manual. Please refer to Appendix A for a complete description/definition of the capitalized terms whenever you see them in this Manual.

If, after reading this document and receiving HIPAA training, you still have questions, please contact LaVonne Shannon in the Department of Personnel and Civil Service, Benefits Office (412) 255-2514.

TOPIC: Group Health Plan and Plan Document
SUBJECT: Process to ensure that the Plan restricts Uses and Disclosures of PHI consistent with the HIPAA regulations to plan sponsors.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan, including benefits which may be either insured or self-insured, is a covered entity under HIPAA. In order for the Plan to disclose PHI to the plan sponsor or to provide for or permit the Disclosure of PHI to the plan sponsor by a Health Insurance Issuer or HMO with respect to the Plan, the Plan will ensure that the plan document restricts Uses and Disclosures of PHI by the plan sponsor consistent with HIPAA requirements, including those relating to Genetic Information for Underwriting Purposes.

In order for the plan sponsor to obtain PHI from the Plan without an Authorization, the plan document will be amended to:

- Describe the permitted Uses and Disclosures of PHI by the plan sponsor;
- Specify that Disclosure is permitted only upon receipt of a written certification by the plan sponsor that the plan document has been amended in accordance with the HIPAA requirements;
- Provide adequate firewalls which identify the employees or classes of employees or other person under the plan sponsor's control who will have access to PHI;
- Provide that the plan sponsor will implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Availability and Integrity of the ePHI it creates, receives, maintains or transmits on behalf of the Plan;
- Ensure that the separation between the Plan and the plan sponsor is supported by reasonable and appropriate Security measures;
- Require that the plan sponsor report to the Plan any Security Incident of which it becomes aware;
- Ensure that any agents, including subcontractors, to receive PHI agree to implement reasonable and appropriate Security Measures to protect the information; and
- Provide an effective mechanism for resolving any issues of non-compliance by the employees or class of employees who will have access to PHI.

The Plan (or a health issuer or HMO with respect to the Plan) may disclose summary Health Information to the plan sponsor without regard to whether the plan documents have been amended, if the plan sponsor requests the summary Health Information for the purpose of:

- Obtaining premium bids from Health Plans for providing health insurance coverage under the Group Health Plan; or
- Modifying, amending or terminating the Group Health Plan.

Additionally, the Plan (or a health issuer or HMO with respect to the Plan) may disclose to the plan sponsor information on whether the Individual is participating in the Plan, or is enrolled in or has disenrolled from a Health Insurance Issuer or HMO without regard to whether the plan document has been amended.

Effective as of the date determined by the Secretary, any disclosure of Summary Health Information provided to the Plan sponsor from a health issuer or HMO with respect to the Plan must not include Genetic Information for Underwriting Purposes.

PROCEDURES:

The Plan will:

- Determine and establish the permitted and required Uses and Disclosures of PHI by the plan sponsor.
- Establish procedures for preventing the improper Uses and Disclosures of PHI by the plan sponsor.
- Implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Availability and Integrity of the ePHI it creates, receives, maintains or transmits.
- Ensure that the separation between the Plan and the plan sponsor is supported by reasonable and appropriate Security Measures.
- Determine the key employees (by job function/description) of the plan sponsor who shall have access to the Plan's PHI.

Reports from third party administrators back to the Plan may contain both aggregated data and individually identifiable data. These practices are intended to continue in the future. To the extent it is necessary to continue to receive Individually identifiable data the Plan will certify to its third party administrators that it has amended its plan document appropriately and disclose to them the identify of the Individuals who are authorized to continue to view this data.

Effective as of the date determined by the Secretary, the Plan sponsor will not accept any disclosure of Summary Health Information provided to the Plan sponsor by a health issuer or HMO with respect to the Plan that includes Genetic Information for Underwriting Purposes.

List of functions performed: Examples of PHI which may be Used or Disclosed

Treatment: None. The Plan does not provide treatment.

Payment: Providing eligibility, enrollment and disenrollment information to insurers and HMOs that provide coverage for Plan participants and providing PHI in the billing, collection, and payment of premiums and fees to such insurers and HMOs.

Health Care Operations: Determining the cost impact of benefit design changes, the disclosure of PHI to underwriters for the purpose of calculating premium rates and providing reinsurance quotes to the Plan, disclosure of PHI to Plan consultants who provide legal, actuarial, and auditing services to the Plan, and use of PHI in general data analysis used in long-term management and planning for the Plan.

Categories of PHI

- Information regarding eligibility, enrollment, disenrollment and change in status in the Plan
- Information relating to claims filed
- Information relating to adjudication of claims appeals
- Participant contributions and premium payments
- Information regarding disputed enrollment or eligibility
- Claim costs, administrative costs, stop-loss premiums and provisions, audit reports
- Risk adjusting and cost-sharing determinations
- Disclosures to government agencies as required by law
- Disclosures to entities or individuals authorized by the Plan participant
- Any other category of PHI that the Privacy Officer deems necessary to carry out Plan functions and which does not violate the HIPAA privacy regulations

PHI may not be used or disclosed for any employment-related decisions, such as hiring, promotion or termination, and PHI may not be used for any employment-related decisions, such as leave of absence, drug testing and compliance with the Americans with Disabilities Act and the Family Medical Leave Act without proper Authorization from the employee.

TOPIC: Designation of a Privacy Officer
SUBJECT: Designation of a Privacy Officer who is responsible for the development and implementation of the Plan's privacy policies and procedures.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has designated a Privacy Officer who is responsible for the development and implementation of the Plan's privacy policies and procedures.

The Privacy Officer will ensure a central point of accountability within the Plan and the City for privacy-related issues. The Privacy Officer is charged with developing and implementing the policies and procedures for the Plan, as required throughout the regulation and for compliance with the regulation generally. The Privacy Officer may be an additional responsibility given to an existing employee of the City.

The Privacy Officer will be available to answer employee questions throughout the employee's employment with the City.

PROCEDURES:

The Privacy Officer will be trained and able to review the Privacy Program. As necessary, the Privacy Officer, or a designee, will:

- Conduct HIPAA privacy Training
- Document privacy policies and procedures
- Keep up to date with privacy developments and modifications to the rules
- Establish employee Sanctions for failure to comply
- Maintain compliance records
- Monitor and respond to employee complaints
- Respond to requests from regulatory agencies
- Establish a system for logging Uses of PHI

The Privacy Officer, or a designee, will be responsible for monitoring the Plan's privacy procedures and practices internally on a periodic basis. The Director, Personnel and Civil Service has been designated as the HIPAA Privacy Officer for the Plan. The Privacy Officer will be assisted in the fulfillment of these responsibilities by the HIPAA Security Officer, the Benefits Manager, and/or the Assistant Director, Personnel and Civil Service (as appropriate).

TOPIC: Mitigation of Harmful Effects of Unauthorized Use or Disclosure of PHI
SUBJECT: Process to mitigate any harmful effect of a Use or Disclosure of PHI in violation of the HIPAA regulations.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will develop and implement procedures to mitigate, to the extent practical, any harmful effect that is known to it. This includes unauthorized Uses or Disclosures of PHI by the Plan or its Business Associates. The Plan will be responsible for mitigating harm when it has actual knowledge of harm even if a deleterious effect cannot be shown.

The Plan will ensure (via its contracting process) that its Business Associates agree to mitigate, to the extent practicable, any harmful effect that is known to those Business Associates of a Use or Disclosure of PHI by a Business Associate in violation of the requirements of the Privacy or Security Rules.

PROCEDURES:

The Plan will take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to the patient or another Individual, and what steps can actually have a mitigating effect in that specific situation.

The Plan will use flexibility and judgment by those familiar with the circumstances to dictate the approach that is the best to mitigating the harm.

If an employee within the firewall becomes aware of an inadvertent misuse or other wrongful disclosure of PHI, the employee, on his or her own or seeking assistance of another within the firewall, will take reasonable measures to end or limit the misuse.

In the event that there is an unauthorized Disclosure of PHI, the Privacy Officer will be notified and steps will be determined to mitigate the effects of the unauthorized Disclosure, depending upon the circumstances of the situation. If, according to the particular circumstances of the misuse or wrongful Disclosure, it is reasonable to do so, the HIPAA Privacy Officer and/or HIPAA Security Officer may evaluate the specific situation and determine if any further corrective action is needed. If a Business Associate's practices or patterns of activity have violated the privacy regulations, then the Plan will to take reasonable steps to cure the violation. If such steps were unsuccessful, the Plan would terminate the contract or if such termination was not feasible, would report the problem to the Secretary of HHS.

TOPIC: Record Retention
SUBJECT: Process for retaining Individual Health Information, including the development, implementation and maintenance of appropriate processes to provide healthcare records as requested.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will maintain all PHI and related documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is later, to meet the applicable requirements of the privacy and/or Security rules. The intent is to ensure member PHI is available so that the Plan can comply with the Individual's requests for an accounting of Disclosures of their PHI. (See also, Accounting (Logging) of Disclosures of Member PHI, Section 8.2)

Business Associate contracts will include contract language that meets the HIPAA record retention requirements, accessibility of records (i.e., for accounting purposes), and how records will be transferred upon termination. (See also, Business Associates and Contracts, Section 3.1).

PROCEDURES:

The Privacy Officer (or a designee) will be responsible for overseeing the process used for record retention. Other managers or personnel may be charged with maintaining healthcare information as required within their area to be HIPAA compliant regarding record retention.

A log for non-Routine Disclosures of Protected Health Information will be developed and maintained.

The contracts of the Business Associates have been amended to ensure that the Business Associates will comply with all aspects of HIPAA Privacy and Security, including record retention.

TOPIC: Reporting of Non-Compliance with the HIPAA Requirements
SUBJECT: A process for filing a complaint with the HHS Secretary when a person believes that the Plan, a Business Associate or other Covered Entity is not complying with the HIPAA requirements.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will support the HHS policy that states that an Individual may file a complaint with the HHS Secretary when such an Individual believes that the Plan is not complying with the HIPAA requirements. The Plan will also allow persons other than the Individual, such as personal representatives, to exercise the rights of the Individual under certain circumstances (e.g., for a deceased Individual).

Any person may become aware of conduct that is in violation of the rule. This can include City employees, the Plan's Business Associates, or other organizations. Complaints can be filed by any person, group, or organization. The person or organization who files the complaint will not be subject to any embarrassing or retaliatory action or threat of action.

PROCEDURES:

Any Individual or organization that becomes aware of conduct by the Plan, its Business Associate(s), or another related Covered Entity that is in violation of the Privacy rule does not have to use the Plan's internal HIPAA complaint process and can file a complaint directly with HHS. This includes the City's employees and their dependents, Business Associates, and accrediting, oversight, and advocacy organizations. The Plan will provide the information necessary for the Individual or organization to contact HHS as part of its Notice of Privacy Practices and also upon further request.

An Individual or organization who believes that an agreement can be reached with the Plan may also use the Plan's HIPAA internal complaint process or other means to seek resolution before filing a complaint with the Secretary. (See, Complaint Process, Sec. 5.4.)

TOPIC: Workforce Sanctions
SUBJECT: Process for applying appropriate Sanctions against the members of the Workforce who fail to comply with the Plan's privacy and security policies and procedures or the HIPAA regulations.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has established policies and procedures regarding disciplinary actions. Sanctions will be implemented for those Individuals who do not follow the outlined policies and procedures. This will be applied to all violations, not just repeat violations.

In addition to internal Sanctions, employees, agents, and contractors of the Plan or the plan sponsor may be advised of civil or criminal penalties for misuse or misappropriation of Health Information. The Plan will inform employees, agents and contractors that violations may result in notification to Law Enforcement Officials and regulatory, accreditation and licensure organizations.

PROCEDURES:

Employees will be made aware of what actions are prohibited and punishable. Training will be provided and expectations will be made clear so Individuals are not sanctioned for doing things which they did not know were wrong or inappropriate.

The Plan will determine what types of sanctions to apply, and may take any action it deems appropriate including suspension or immediate termination without notice or warning. Nothing in this Manual is intended to alter the at-will status of employment with the City. The City and the Plan reserve the right to terminate employment with or without cause and with or without advance notice.

The City of Pittsburgh Group Health Plan reserves the right to proceed directly to termination of employment. However, where appropriate, and in the sole discretion of the HIPAA Privacy Officer, termination of employment may be preceded by an oral/or written warning(s).

Managers are responsible for ensuring that the HIPAA Privacy Officer is notified of workforce members who fail to comply with the privacy policies. The Privacy Officer will assist managers with the necessary information to appropriately apply disciplinary action, including notification to law enforcement officials and other regulatory organizations.

Please refer to section 9.1.3 of these HIPAA Policies and Procedures for Security Sanction procedures.

TOPIC: Safeguards
SUBJECT: Creating, implementing and maintaining reasonable processes and safeguards for the protection of PHI

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will have appropriate Administrative, Technical, and Physical Safeguards in place to protect the privacy of PHI and the Confidentiality, Integrity, and Availability of ePHI. The Plan will reasonably safeguard PHI from any intentional or unintentional Use or Disclosure that is in violation of the HIPAA Privacy or Security Rule requirements.

The Plan will have reasonable and appropriate Administrative, Physical, and Technical Safeguards in place to protect against the inadvertent Disclosure of PHI to persons other than the intended recipient.

PROCEDURES:

The Plan will determine what types of safeguards to apply. The list of appropriate safeguards will include:

- All documents containing PHI are required to be disposed in shredding bins,
- All doors accessing areas where PHI is stored are required to remain locked after business hours, or when the office is unattended,
- All file cabinets housing such records are required to be locked after business hours,
- Personnel who are authorized to key or pass code access to PHI shall be limited,
- All computer system access is password protected,
- Ensure that documents containing PHI on desk tops and work stations are not in plain view of passers-by,
- Identification of workstations used to access PHI,
- Identification of other physical safeguards put in place to minimize the risk of unauthorized access to PHI,
- Location(s) of workstations,
- Privacy screens around work areas,
- Other access controls or physical protections (i.e., locking devices on workstations),
- Automatic data backups,
- Firewalls,
- Automatic updates to anti-virus software; and/or
- External monitoring processes.

Additional safeguards applying to ePHI may be found in Sections 9 through 11 of this HIPAA Policies and Procedures document.

TOPIC: Authorizations for Uses and Disclosures of PHI
SUBJECT: Process for authorizing Uses and Disclosures of PHI when it is not used for Payment, Treatment or operations, or non-Routine, permissible Uses and Disclosures of PHI.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

Authorizations are required for the Use and Disclosure of PHI for purposes other than the permitted Uses and Disclosures specified in the Privacy Rule.

The Plan will obtain the Individual's permission prior to using or disclosing PHI when it is not used to carry out Routine (Payment, Treatment or Health Care Operations) or non-Routine Uses and Disclosures. Except as listed in the Uses and Disclosures of PHI Policy, Section 8.1, the Plan will not use or disclose PHI without an Authorization. When the Plan receives a properly authorized request for the release of PHI, it will adhere to the terms of the Authorization.

The Plan will document and retain any signed Authorizations and will provide the Individual with a copy of the signed Authorization.

PROCEDURES:

The permissions granted in the Authorization should not be acted upon if the Authorization has been revoked or if it has expired. The Authorization will be documented and retained for a period of six (6) years after it was created or expired, whichever date is later.

When the need for an authorization arises, the Plan will get a signed authorization from the Individual whose PHI is going to be used or disclosed. Only the Plan's standard authorization form should be used. The Individual will be provided with a copy of the Authorization form and asked to sign it. Signing an Authorization form is voluntary and the Individual may refuse to sign it. A copy of the signed Authorization will be provided to the Individual. The Individual may revoke the Authorization, in writing, at any time

A signed copy of all authorization and revocation forms must be sent to City of Pittsburgh's Personnel Department, Benefits Office. The Personnel Department, Benefits Office retains copies of all signed forms.

When the Personnel Department, Benefits Office receives a request for a revocation of an authorization, it first must research to see if the revocation can be honored. Then the Personnel Department, Benefits Office will respond in writing to the individual stating if the authorization has been revoked and, if not, the reason why. Copies of this letter are retained with the signed revocation request form. The Personnel Department, Benefits Office is also responsible for contacting the person/entity listed as the "person receiving the PHI" on the initial authorization form and informing them of the revocation.

Most Uses and Disclosures requiring an Authorization will be handled by the Plan's vendors. Authorizations acquired by Business Associates will need to be revoked via the Business Associate and not by the Plan.

A copy of the Plan's Authorization Form is attached as Appendix B.

TOPIC: Business Associates and Contracts
SUBJECT: Contracting issues to assure that Business Associates comply with the Plan's HIPAA policies and procedures.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan's Business Associates are required to provide satisfactory assurances that they will safeguard and maintain the Confidentiality, Integrity and Availability of the PHI of the Plan's Individuals and only use and disclose PHI for the purposes for which it was provided and in accordance with the HIPAA Privacy and Security Rules.

PROCEDURES:

Existing and new relationships with the Plan's service providers have been and continue to be reviewed to determine if the relationship requires the Use and/or Disclosure of PHI and thus, whether the entity is a Business Associate. A current listing of Business Associates has been compiled and is attached to this Policies and Procedures as Appendix C. This listing will be reviewed periodically to determine whether any updates to the listing are required.

Business Associates are required to sign a written contract that provides satisfactory assurances that they will adhere to the Plan's HIPAA practices. The Plan requires its Business Associates to determine the Minimum Necessary type and amount of PHI required to perform the services under the Agreement and to represent to the Plan that it has requested the Minimum Necessary PHI for the stated purpose. The Plan relies on the professional judgment of its Business Associates to determine the type and amount of PHI necessary for their purposes.

The Privacy Officer, Security Officer, or a designee, will monitor the return or destruction of PHI Used, created or obtained by the Business Associate upon termination of the contract (or the extension of protection if not returned or destroyed).

The Privacy Officer, Security Officer, or a designee, will ensure that any complaints regarding privacy violations by Business Associates are reviewed. If the Privacy Officer or Security Officer is aware of a pattern or practice that is a material violation of the Business Associate's duties with regard to privacy, the Privacy Officer, Security Officer, or a designee, will take reasonable steps to end the violation. If such steps are unsuccessful, the Privacy Officer or Security Officer will determine whether termination of the agreement is feasible. If not, the Privacy Officer or Security Officer will report the violation to HHS.

TOPIC: Disclosure of PHI to Plan Sponsor
SUBJECT: Requirements concerning when and how the Plan may disclose PHI to the plan sponsor.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will not disclose PHI to the plan sponsor, except in the manner and for the purposes specifically permitted under the Privacy Rule. The Plan will only disclose PHI to the plan sponsor if one of the following applies:

- The Plan receives written Authorization from an Individual to disclose PHI to the plan sponsor;
- The Plan discloses information to the plan sponsor on whether an Individual is participating in the Health Plan;
- The Plan provides the plan sponsor with PHI in the form of Summary Health Information for the purpose of obtaining premium bids from Health Insurance Issuers;
- The Plan provides the plan sponsor with PHI in the form of Summary Health Information for the purpose of assessing, modifying, amending or terminating the Health Plan; or
- The Plan receives certification from the plan sponsor that the plan documents have been modified as required by the Privacy Rule, and the Uses and Disclosures of PHI by the plan sponsor will be restricted to Plan Administration Functions performed by the plan sponsor on behalf of the Plan in accordance with the plan document.

The Plan will require certification from the plan sponsor that the plan sponsor will not use PHI for any employment-related decisions and that the plan documents have been amended as required before disclosing PHI to the plan sponsor.

The Plan has included a separate statement in its Notice of Privacy Practices informing Individuals that PHI may be disclosed to the plan sponsor. The Plan will only disclose the Minimum Necessary amount and type of PHI to the plan sponsor.

PROCEDURES:

Effective October 15, 2009, the following positions are within the firewall:

- Director, Personnel and Civil Service
- Assistant Director, Employee Compensation
- Benefits Manager
- Group Benefits Coordinator
- Assistant Director, Personnel and Civil Service

The access to, use and disclosure of PHI by the individuals named above are restricted to the category or categories of PHI required to carry out their duties and job responsibilities.

The City of Pittsburgh Personnel Department, Benefits Office (the "Benefits Office") is the primary contact for employees' health benefits related inquiries. Employees within the Firewall typically have access to PHI via formal claims appeal process as well as through day to day telephone calls, e-mails or personal visits from employees with benefits related issues. The Benefits Office also receives inquiries from employees and provides assistance which generally includes such tasks as assisting participants with obtaining information regarding status of claims filed and other related issues.

TOPIC: Granting Levels of Access to PHI

SUBJECT: Process to identify those persons or classes of person in the Plan's Workforce who need access to PHI to carry out their duties. This includes the technical Security measures to protect information and to control Individual access to information.

EFFECTIVE DATE: April 14, 2003

REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will identify persons or classes of persons employed by the City who need access to PHI to carry out their duties. The Plan will make a reasonable effort to limit the access of such persons or classes to PHI based on Minimum Necessary requirements.

The Plan will maintain Administrative, Physical and Technical Security Measures to protect PHI and to control Individual access to information, including both access and authorization controls.

The Plan will have formal, documented termination procedures and instructions that include appropriate Security measures for the termination of an internal/external User's access.

PROCEDURES:

The Privacy Officer, Security Officer, or a designee, will determine which Individuals or classes of Individuals can access PHI as part of their job functions, and identify the categories of PHI to which these access rights apply. The Privacy Officer, Security Officer, and/or a designee will review requests for non-Routine Disclosures on an Individual basis, using set criteria.

TOPIC: Individual's Rights to Access PHI
SUBJECT: Process for assuring that members have the right of access to their PHI.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has implemented policies and procedures to ensure Individual's privacy rights as required by and specified in the HIPAA Privacy Rule. Individuals have the right to request to inspect or obtain a copy of their Protected Health Information ("PHI") in the Designated Record Set.

Individuals in the Plan have the rights to:

- Receive a paper copy of the Plan's Notice of Privacy Practices ("Notice"), even if the Individual has agreed previously to receive the Notice electronically;
- Request restrictions on the Uses and Disclosures of Protected Health Information;
- Request to receive confidential communication by an alternative means or at an alternative location if appropriate cause is shown;
- Access documents in the Designated Record Set for inspection and/or copying;
- Request to amend documents in the Designated Record Set that are inaccurate or incomplete; and
- Obtain an accounting of certain Disclosures of their PHI.

The Plan adheres to policies and procedures developed and implemented to ensure Individual privacy rights.

PROCEDURES:

The Plan will require and inform Individuals that requests for access to PHI must be made in writing. When a request for access to PHI is received, it will be acted upon according to the following timeframes:

- Within thirty (30) days if the requested information is maintained and accessible on site (information maintained with the City's Benefits Office); or
- Within sixty (60) days if the requested information is maintained offsite.

The Plan will document the records that comprise the designated record set that is subject to access requests and maintains such records for a period of six (6) years from the date they were created or were last in effect, whichever is later. The Plan will maintain the titles of the persons/offices responsible for receiving and processing access requests for a period of six (6) years.

When a request for access is accepted (in whole or in part):

To the extent possible, the Plan will grant access to PHI for which there are no grounds to deny access. The Plan will inform the Individual and provide the access requested, within the timeframes above. The timeframes stated above may be extended one time for no more than thirty (30) days. If the extension is necessary, the Plan will provide the Individual, within the timeframes above, a written statement that specifies the reason(s) for the delay and the date by which the Individual may expect to receive a decision on the request to access the PHI.

In lieu of providing access, the Plan may provide a summary of the requested PHI for an additional charge if the Individual agrees to the summary and to the additional fee. The Plan and the Individual will arrange a mutually convenient time and place for the Individual to inspect and/or obtain a copy of the requested PHI. The Plan will mail a copy of the requested PHI if the Individual prefers this method of obtaining a copy.

When the Plan denies a request for access (in whole or in part):

The Individual is given a statement written in plain language that includes:

- The reasons for the denial decision;
- If applicable, the Individual's right to a review of the decision with an explanation of how to exercise this right; and
- A description of how the Individual may file a complaint with the Plan and HHS, including the title and telephone number of a Plan contact person.

If the denial is reviewable and the Individual requests such a review, the Plan will designate a licensed health care professional, not involved in the original denial decision, to serve as a reviewing official. Upon receipt of a review request, the Plan will promptly refer the denial to the reviewing official for reevaluation. The Plan will provide written notice to the Individual of the reviewing official's determination.

If the Plan denies access because it does not maintain the PHI requested but knows where the requested PHI is maintained, the Plan will inform the Individual of where to direct the request.

TOPIC: Individual Request to Amend PHI
SUBJECT: Process for assuring member's rights to have the Plan amend their PHI.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

Individuals have the right to request amendment of incorrect or incomplete PHI contained in a Designated Record Set.

PROCEDURES:

The Plan will require and inform Individuals that requests for amendment of their PHI must be made in writing and must include a reason to support acceptance of the amendment.

When a request for amendment of PHI is received, it will be acted on within sixty (60) days. If necessary, this timeframe may be extended for thirty (30) days. The Individual requesting the amendment will be informed in writing of the reason(s)for the delay and the date by which action will be taken on the request. The extension notice will be provided within sixty (60) days of receipt of the original request.

The Plan will document the titles of the persons responsible for receiving and processing requests for amendment and retain such documentation for a period of six (6) years.

When a request for amendment is denied:

The Individual is given a notice written in plain language that:

- Includes a permissible basis for denial (for example, that the information requested was not created by the Plan, is accurate and complete, is not part of the record, or may not legally be changed)
- Informs the Individual of the right to submit a statement of disagreement, and how to file the statement;
- States that if the Individual does not file a statement of disagreement the Individual may request that the Plan provide the request for amendment and the denial in any future release of the disputed PHI; and
- Includes a description of the procedure to file a complaint with the Plan or HHS.

If the Individual chooses to write a statement of disagreement with the denial decision:

- The Plan may write a rebuttal statement and will provide a copy to the Individual; and
- The Plan will include the request for amendment, denial letter, statement of disagreement, and rebuttal (if any), with any future disclosures or the disputed PHI.

If the Individual does not choose to write a statement of disagreement with the denial decision, the Plan is not required to include the request for amendment and denial decision letter with future disclosures of the disputed PHI unless requested by the Individual.

When a request for amendment is accepted (in whole or in part):

The Plan will identify the record(s) that are the subject of the amendment request and will append the amendment to the record(s). The Plan will inform the Individual that his or her request for amendment has been accepted and request the identification of and permission to contact other individuals or health care entities that need to be informed of the amendment(s).

The Plan will make reasonable efforts to provide the amendment within a reasonable time to the persons/entities identified by the Individual as well as persons and Business Associates whom the Plan knows have the disputed PHI and may rely on it to the Individual's detriment.

Receipt of notification of amendment from other Covered Entities

When the Plan receives notification from another Covered Entity that an Individual's PHI has been amended:

- The Plan will ensure that the amendment is appended to all applicable records of the Individual, and
- The Plan will inform its Business Associates that may use or rely on the Individual's PHI of the amendment and require them to make the necessary corrections.

TOPIC: Individuals' Rights to Request Privacy Protection for PHI
SUBJECT: Process for assuring that member's rights to request privacy protection for PHI are met.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

Individuals have the right to request restrictions on how their PHI is Used and/or disclosed for Treatment, Payment and Health Care Operations. An Individual may request confidential communications at any time.

PROCEDURES:

Individuals are informed of their right to request restrictions on the use and disclosure of their PHI in the Plan's Notice of Privacy Practices ("Notice"). All requests by Individuals for restrictions on the use and disclosure of their PHI must be made in writing and forwarded to the Privacy Officer or designee for approval:

The City of Pittsburgh
Department of Personnel and Civil Service
Benefits Office
City-County Building
414 Grant Street
Pittsburgh, PA 15219

Individuals who desire their PHI to be communicated in an alternative manner, or location other than the Plan would otherwise use, will be required to specify the alternative location or other method of communication. The Individual will be required to clearly state that the restriction is necessary to prevent a disclosure that could endanger the Individual.

The Plan will not refuse to accommodate such requests unless the request imposes an unreasonable administrative burden on itself or its Business Associates.

When a request for restriction(s) is accepted:

The Individual will be informed of any potential consequences of the restriction, including that the Plan is not required to comply with the agreed-upon restriction(s) in emergency treatment situations when the restricted PHI may be needed for treatment.

The Plan and its Business Associates will not use or disclose PHI inconsistent with the agreed restriction. The use and/or disclosure of PHI will be consistent with the status of the restriction in effect on the date it is used or disclosed

Written documentation of the agreed-to restriction will be maintained for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

When a request for restriction(s) is denied:

The Individual will be given the opportunity to discuss his or her privacy concerns, if desired, and efforts will be made to assist the Individual in modifying the request for restrictions to accommodate his or her concerns and obtain acceptance by the Plan.

TOPIC: Complaint Process
SUBJECT: A process for filing a complaint with the Plan when a person believes that the Plan, a Business Associate or other Covered Entity, is not complying with the HIPAA requirements.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will have a means of receiving complaints concerning violations of the HIPAA rules and regulations and the Plan's HIPAA practices. The Plan will designate a contact person or office that is responsible for receiving complaints related to the Plan's compliance with the HIPAA regulations. This person or office will be responsible for providing further information about areas covered under the Plan's Notice and for maintaining a record of the complaints that are filed and a brief explanation of their resolution, if any.

PROCEDURES:

The Plan will direct complaints centrally to the Director, Personnel and Civil Service (the HIPAA Privacy Officer) in the Benefits Office who will have primary responsibility for receiving and responding to member complaints. The Privacy Officer, in his or her discretion, may delegate day-to-day responsibility for receiving complaints to another Workforce member in the Benefits Office

The HIPAA Privacy Officer, or designee, will be responsible for logging the complaints received and maintaining a record of those complaints, along with a brief explanation of their resolution, if any.

TOPIC: Notice of Privacy Practices
SUBJECT: An Individual has a right to adequate notice of the Uses and Disclosures of PHI that may be made by the Plan, and of the Individual's rights and the Plan's legal duties with respect to PHI.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan's privacy practices, designed to protect the privacy, Use and Disclosure of PHI, are described and clearly delineated in the Plan's Notice or Privacy Practices ("Notice") which was developed and is used in accordance with the Privacy Rule.

PROCEDURES:

The Notice is distributed to all new Individuals at enrollment. All Individuals will receive a revised Notice within sixty (60) days of any material revision to the Notice. The Notice is provided to the named Individual or employee for the benefit of all dependents.

The Notice is available to anyone who requests it. Individuals have the right to receive a paper copy of the Notice, even if they previously agreed to receive the Notice electronically.

All current Individuals are notified at least once every three years of the availability of the Notice and provided with instructions on how to obtain it.

The Notice will be revised as needed to reflect any changes in the Plan's privacy practices. When revisions to the Notice are necessary, all current Individuals and Workforce members who perform Plan functions will receive a revised copy of the Notice.

The Privacy Officer will retain copies of the original Notice and any subsequent revisions for a period of six (6) years from the date of its creation or when it was last in effect, whichever is later.

The Notice will be made available through the City's Benefits Office and will be displayed on the City's intranet site(s).

A copy of the Notice is attached here as Appendix E.

TOPIC: Minimum Use of PHI
SUBJECT: The Plan will make reasonable efforts to ensure that the minimum amount of PHI necessary to accomplish the intended purpose of the Use or Disclosure is Used or Disclosed.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

For any disclosures that are made a Routine and recurring basis, the Plan will make reasonable efforts to limit the PHI disclosed to the amount minimally necessary to accomplish the intended purpose for the Use, Disclosure, or request. For all other Disclosures, the Plan will limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which Disclosure is sought, and will review requests for Disclosure on an Individual basis in accordance with such criteria. The Plan will reasonably safeguard PHI from any intentional or unintentional Use or Disclosure that is in violation of the standards, Implementation Specification or other requirements.

The following situations are exceptions to the Plan's Minimum Necessary standards:

- Disclosures or requests by a health provider for Treatment;
- Uses or Disclosures made pursuant to the Individual's Authorization;
- Uses and Disclosures made to the Individual to whom the PHI applies as permitted or required by applicable regulations
- When the Secretary of HHS requests access to the information to ensure compliance or investigate a complaint;
- Uses or Disclosures that are Required by Law; or
- Use or Disclosures that are required to comply with requirements of applicable regulations.

The Plan will make determinations of Minimum Necessary Use based on the types of people who are to have access to designated categories of information and the conditions, if any, of that access. The Plan will take appropriate means for protecting the privacy of Individuals' information.

PROCEDURES:

The Plan will implement procedures to limit the Use and Disclosure of PHI to the minimum information reasonably necessary to achieve the purpose of that type of Use or Disclosure.

The Plan will determine who needs to have access to PHI and identify the categories of PHI to which access is needed and conditions appropriate to such access. For Routine and permissible Uses or Disclosures of PHI, the Plan will consider the minimum information reasonably necessary to achieve the purpose of that type of Use or Disclosure and will make every effort to ensure consistency. What is reasonable to comply with the Minimum Use of PHI Policy will vary based on the circumstances. The Plan will use discretion to determine what is the Minimum Necessary in each situation.

When it is practical, the Plan may use selective copying or Disclosure of relevant portions of a record, report, or other information.

TOPIC: Training Workforce Regarding Protection of Health Information
SUBJECT: Process for Training members of the Workforce on the policies and procedures with respect to PHI as required by regulations.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan and/or the City will train members of its Workforce on its policies and procedures with respect to PHI as required under applicable regulations as necessary and appropriate for the members of the Workforce to carry out their job function.

Training will be provided to each appropriate member of the Workforce on privacy, Confidentiality and Security requirements that are applicable to their work. Each new member of the Workforce will receive the Training within four (4) weeks after joining the Workforce. The Training is designed to address the types of issues the employees will confront in performing their obligation as well as address general privacy issues and to educate Workforce members as to the Plan's policies and procedures.

When there is a material change in the privacy policies and/or procedures, each member of the Workforce whose function is affected by the change will be trained within four (4) weeks after the change becomes effective.

PROCEDURES:

The Privacy Officer, Security Officer, or designee will determine a method of Training to train appropriate staff. This may include memos, emailed notices, self-learning packets, review of policies and procedures, or another appropriate method. The information can be taught at meetings, one-on-one Training or by self-teaching. The person responsible for the Training session will also be responsible for providing documentation of the Training to the Privacy Officer and/or Security Officer.

Training will be provided to each appropriate member of the Workforce on privacy and security requirements that are applicable to their work. This will include all employees behind the firewall. (See also, Disclosure of PHI to Plan Sponsor, Section 4.1). Training will be provided to each appropriate member of the Workforce on privacy, Confidentiality and Security requirements that are applicable to their work.

On-going Training will be conducted within four (4) weeks whenever there is a material change to the HIPAA privacy requirements or to the Plan's policies and procedures. The delivery method for such on-going Training may vary and/or be revised as the circumstances allow. New employees entering into roles/functions within the firewall will be logged in and trained within four (4) weeks from the date they begin working with PHI as part of their designated job function.

The Plan will document its Training in written or electronic form and maintain such documentation for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

TOPIC: Uses and Disclosures of Protected Health Information (PHI)
SUBJECT: Process to identify the permitted Uses and Disclosures of the Plan's PHI.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will not use or disclose PHI except as permitted or required by the HIPAA rules and regulations or in this policy.

I. Routine Uses and Disclosures of PHI

The Plan may:

- Use or disclose PHI to carry out its own Payment, or Health Care Operations functions.
- Disclose PHI to the Individual to whom the PHI applies.
- Disclose PHI to another Covered Entity for Payment activities of the entity that receives the information.
- Disclose PHI for Treatment activities for a Health Care Provider
- Disclose PHI to another Covered Entity for Health Care Operations activities of the entity that receives the information, if both entities have or had a relationship with the Individual who is the subject of the PHI being requested and the Disclosure is for purposes of quality assessment and improvement, case management, care coordination, contacting Individuals regarding Treatment alternatives, reviewing Health Plan performance, detecting Health Care fraud and abuse, and any other purposes permitted by applicable regulations.

II. Non-Routine Uses and Disclosures of PHI

The Plan will log all requests for Disclosures of non-Routine permissible PHI for both internal and external Disclosures. An Authorization or opportunity to agree or object will not be required for the following categories of Use or Disclosure of PHI:

(a) Required by law. The Plan may Use or disclose PHI to the extent that such Use or Disclosure is Required by Law and the Use or Disclosure complies with and is limited to the relevant requirements of such law.

(b) Public Health Activities. The Plan may disclose PHI for public health activities to the following:

- A Public Health Authority that is 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 such as birth or death, and the

conduct of public health surveillance, public health investigations, and public health interventions; or to an official of a foreign government agency that is acting in collaboration with a Public Health Authority.

- A Public Health Authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
- A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA- regulated product or activity for which that person has responsibility, for the purposes of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity.
- A person who will have been exposed to a communicable disease or will otherwise be at risk of contracting or spreading a disease or condition where the law authorizes notification as necessary in the conduct of public health intervention or investigation.

(c) Victims of abuse, neglect or domestic violence. The Plan may disclose PHI about an Individual whom the Plan reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority. The Plan will disclose PHI regarding such Individual when the Disclosure is Required by Law, when the Individual agrees to the Disclosure, or when the Disclosure is authorized by statute or regulation.

(d) Health oversight activities. The Plan may disclose PHI to a health oversight agency for oversight activities authorized by law for appropriate oversight of the Health Care system, government benefit programs for which Health Information is relevant to beneficiary eligibility, government regulatory programs for which Health Information is necessary for determining compliance with program standards or entities subject to civil rights law for which Health Information is necessary in determining compliance.

(e) Judicial and administrative proceedings. The Plan may disclose PHI in the course of any judicial or administrative proceeding in response to a court or administrative tribunal order provided that only PHI expressly authorized by the order is disclosed; or in response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal if satisfactory assurances, as provided for in the regulation, are received by the Plan. The Plan will prohibit the parties from using or disclosing PHI for any purpose other than the litigation or proceeding and will require the return of the PHI, including all copies made, at the end of the litigation or proceeding.

(f) Law enforcement purposes. The Plan may disclose PHI to a Law Enforcement Official for the following purposes:

- When the subject of the Disclosure is an Individual who is or is suspected to be a victim of a crime, abuse, or other harm.
- The reporting of certain types of wounds or other physical injuries
- A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer or a grand jury subpoena.
- An administrative subpoena or summons, a civil or an authorized investigative demand when the information sought is relevant to a legitimate law enforcement

inquiry. The request must be specific and limited in scope to the extent reasonably practicable for the purpose for which the information is sought.
- Limited information for identification and location purposes will be disclosed by the Plan for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person.
- About an Individual who has died, for the purpose of alerting law enforcement of the death of the Individual, if the Plan has a suspicion that such death resulted from criminal conduct.
- Pursuant to the Plan's good faith belief that the Disclosure constitutes evidence of criminal conduct that occurred on Plan or plan sponsor premises.

(g) To avert a serious threat to health or safety. The Plan may use or disclose PHI, based on a good faith belief that it is necessary to prevent or lessen a serious imminent threat, including to the target of the threat, or is necessary for law enforcement authorities to identify or apprehend an Individual under specified circumstances.

(h) Specialized government functions. Subject to certain conditions, the Plan may disclose PHI for certain military and veterans' activities, national security and intelligence activities, and to correctional institutions, as specified in applicable regulations.

(k) Worker's Compensation. The Plan may disclose PHI to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work related injuries or illness.

III. Uses and Disclosures for which an Authorization is required

Except as listed in Sections I and II of this policy, the Plan will not use or disclose PHI without securing the Individual's prior written Authorization. When the Plan receives a request for PHI, the Plan will adhere to the terms of the Authorization, to the extent an Authorization was necessary to permit the Disclosure.

IV. Personal Representatives

If a person has the authority under applicable law to act on behalf of an Individual who is an adult or an emancipated minor in making decisions related to PHI, the Plan will treat such person as a personal representative with respect to PHI. If a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an Individual who is an unemancipated minor in making decisions related to PHI, the Plan will treat such person as a personal representative of an unemancipated minor.

The Plan will, consistent with State or other applicable law, provide a right of access to PHI of an unemancipated minor to either a parent, guardian, or other person acting *in loco parentis*, as the personal representative of the unemancipated minor, or the unemancipated minor, or both.

V. Access to Records

The Plan will permit access by the Secretary of HHS during normal business hours to its books, records and accounts and other sources of information, including PHI, that are pertinent to ascertaining compliance with the privacy requirements. If such information is in the exclusive possession of another person, institution or entity that fails or refuses to furnish the information, the Plan will certify and set forth the efforts it made to obtain the information.

VI. Other Requirements Relating to the Uses and Disclosures of PHI

For Payment Purposes: The Plan shall not use or disclose PHI that is Genetic Information for Underwriting Purposes.

For Health Care Operations Purposes: If the Plan receives PHI for the purpose of premium rating or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the Plan, the Plan may only use or disclose such PHI for such purpose or as may be Required by Law, subject to the prohibition against using or disclosing PHI that is Genetic Information for Underwriting Purposes.

PROCEDURES:

The Plan will disclose or Use PHI or any categories of PHI only to the extent and for the purposes described in this policy. The Plan will not use or disclose PHI that is Genetic Information for Underwriting Purposes.

The Plan will log all non-Routine Disclosures and will maintain all written Authorizations submitted by Individuals in a secure, designated location within the Human Resources Department, Benefits Office. The log will include the specific type of information disclosed (i.e., demographic, Health Information), the purpose, the mode, and the category of recipients to whom the information is being given.

The Privacy Officer, or a designee, will be responsible for maintaining and updating the log of Disclosures of PHI. Updates will be done as new and/or changes in Disclosures occur.

TOPIC: Accounting (Logging) of PHI Disclosures
SUBJECT: Process for logging and providing an accounting of all requests for Uses and Disclosures of PHI to the extent required by applicable regulations.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will develop and maintain a log that provides for a written accounting of Disclosures of PHI. This will support an Individual's right to receive an accounting of Disclosures of PHI made by the Plan for a period of up to six (6) years prior to the date on which the accounting is requested, except an accounting will not be given for the following Disclosures:

(a) To carry out Treatment, Payment and Health Care operations;
(b) To Individuals of PHI about themselves;
(c) For national Security or intelligence purposes;
(d) To correctional institutions or Law Enforcement Officials;
(e) That occur prior to April 14, 2003;
(f) Those made pursuant to the Individual's Authorization; or
(g) Those that are incident to a permitted or required Use or Disclosure.

An Individual may request an accounting of Disclosures for a period of time less than six (6) years from the date of the request.

The Plan will temporarily suspend an Individual's right to receive an accounting of Disclosures to a health oversight agency or Law Enforcement Official for the time specified by such agency or official, if the agency or official provides with a written Statement that such an accounting to the Individual would be likely to impede the agency's activities and specifying the time for which a suspension is required.

The Plan will require its Business Associates to agree to maintain a log of the elements regarding Disclosures of PHI for which an accounting may be required.

Upon termination of the Business Associate Agreement, the Plan will require that the Business Associate maintain all logs that contain the accounting of PHI Disclosure or transfer them to the Plan or a third party designated by the Plan.

PROCEDURES:

The accounting will provide the Individual with a written account of all applicable Disclosures of PHI that occurred during the six (6) years prior to the date of the request for an accounting (or a shorter time period at the request of the Individual), including Disclosures to or by Business Associates of the Plan and will include for each Disclosure:

- The date of the Disclosure
- The name of the entity or person who received the PHI and, if known, the address of the entity or person.
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure.

If during the period covered by the accounting, the Plan has made multiple Disclosures of PHI to the same person or entity for a single purpose, the Plan will provide the following additional information:

- The frequency, periodicity, or number of the Disclosures made during the accounting period; and
- The date of the last Disclosure during the accounting period.

The Plan will respond to the Individual's request for an accounting no later than 60 days after receipt of the request. If the Plan is unable to provide the accounting within 60 days, the Plan may extend the time to provide the accounting by no more than 30 days. Prior to the expiration of the initial 60-day period, the Plan will provide the Individual with a written statement of the reasons for the delay and the date by which the Plan will provide the accounting. The Plan may only have one extension of time for action.

The Plan will document and retain the information supplied according to this policy and the written accounting that is provided to the Individual.

TOPIC: Security Management Process
SUBJECT: Implement policies and procedures to prevent, detect, contain and correct Security violations

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will implement policies and procedures to prevent, detect, contain and correct Security violations. These policies will include the following HIPAA Implementation Specifications:

- 9.1.1 Risk Analysis – an accurate and thorough assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of the Plan's ePHI will be conducted.
- 9.1.2 Risk Management – sufficient Security measures to reduce the risks and vulnerabilities to the Plan's ePHI to a level sufficient to comply with the HIPAA Security Rule will be implemented.
- 9.1.3 Sanctions – appropriate Sanctions against Workforce members who fail to comply with these policies and procedures will be applied.
- 9.1.4 Information System Activity Review – records of Information System activity will be regularly reviewed.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

9.1.1 Risk Analysis

As part of its initial HIPAA Security Rule risk analysis, the Plan assessed the technical and non-technical components of its Security environment as they related to ePHI, including hardware, software, system interfaces, data and information and people. All Information Systems that house electronic PHI, including all hardware and software that are used to collect, store, process, or transmit electronic PHI were identified. Functions and ownership and control of Information System elements were analyzed and verified. The Plan then reviewed and made a reasoned, well-informed and good-faith determination to implement all applicable standards and Implementation Specifications under the HIPAA Security Rule.

A risk analysis summary was created to summarize the findings of the risk analysis. This summary will be maintained by the Security Officer for a period of not less than six (6) years from the date it was completed or last updated.

The risk analysis summary will be reviewed periodically to assess the Plan's compliance with the Security Rule and will be updated as may be necessary. (See also, Evaluation Policy, Section 9.8).

9.1.2 Risk Management

The Plan has analyzed the data collected during the risk analysis and identified the risks and vulnerabilities of any ePHI it stores, processes or transmits.

The Plan will implement reasonable and appropriate Security measures to reduce risks to the Confidentiality, Integrity and Availability of ePHI to a reasonable and appropriate level, taking into consideration the Plan's size, complexity, technical capabilities, risk analysis and the costs of Security measures.

All Security measures which are implemented and/or adopted by the Plan will be documented and the effectiveness of those Security measures will be reviewed and updated as part of the Security Officer's periodic evaluations of the Plan's Security environment.

9.1.3 Sanctions

The Plan has established policies and procedures regarding disciplinary actions which are communicated to employees, agents, contractors and other persons under the Plan's direct control. The Plan will make employees, agents, and contractors aware that violations may result in notification to Law Enforcement Officials and regulatory, accreditation, and licensure organizations and will be advise employees, agents, and contractors that civil or criminal penalties may apply for the misuse, Disclosure or misappropriation of Health Information.

Sanctions will be implemented for those Workforce members who do not follow the outlined policies and procedures. This will be applied to all violations, not just repeat violations. These Sanctions will be supported, and may be supplemented in the Plan's Business Associate agreements.

Training will be provided and expectations will be made clear so Workforce members are not sanctioned for doing things which they were not aware were wrong or inappropriate.

(Please refer to section 1.7 for further details on specific Sanction procedures.)

9.1.4 Information Systems Activity Review

The Security Officer (or his or her designee) will be responsible for coordinating the Information System activity record review as it relates to the Plan's ePHI. Information system activity will be reviewed periodically to detect or correct Security violations.

The City or the Plan maintains the following:

(a) Event logs (including date and time-stamping of data changes);
(b) Security Incident tracking logs (including flagging of unauthorized attempts to access data); and/or
(c) Other internal Security controls and monitoring tools.

Workforce members will be informed that records of Information System activity may be reviewed and can be used to investigate causes of reported or suspected Security Incidents or Security violations.

TOPIC: Assigned Security Responsibility
SUBJECT: Designation of a Security Officer

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has identified and designated a Security Officer who is responsible for the development and implementation of the Plan's Security policies and procedures.

The Security Officer ensures a central point of accountability within the Plan for Security-related issues. The Security Officer is responsible for developing and implementing the policies and procedures for the Plan and for compliance with the HIPAA Security Rule requirements generally. The role of Security Officer may be an additional responsibility given to an existing employee of the Plan.

PROCEDURES:

The Security Officer will be trained and responsible for reviewing the Plan's Security Program. The Security Officer coordinates the Plan's efforts across to identify key Security initiatives and standards including virus protection, Security monitoring, intrusion detection, and physical access control and Security of Health Information held by the Health Plan.

The Security Officer's responsibilities will be documented in a job description. The Security Officer, or a designee, will be responsible for:

(a) Conducting or overseeing employee Training (as it relates to the HIPAA Security requirements),
(b) Establishing employee Sanctions for failure to comply with the Security Rule,
(c) Maintaining compliance records, and
(d) Monitoring the Plan's Security procedures and practices internally on a periodic basis and implementing changes as necessary.

The Director of CIS has been designated to serve as the HIPAA Security Officer for the Plan. This designation has been communicated to the Plan's Workforce.

TOPIC: Workforce Security
SUBJECT: Ensuring appropriate access and preventing inappropriate access to ePHI

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan's policies and procedures are designed to ensure that all members of the Workforce have appropriate access to ePHI and to prevent those members of the Workforce who do not require access to ePHI from obtaining such access. These policies will include addressing the following HIPAA Implementation Specifications:

- 9.3.1 Authorization and/or Supervision (A) – procedures for the Authorization and/or supervision of Workforce members who work with ePHI or in locations where it may reasonably be anticipated to be accessed will be adopted.
- 9.3.2 Workforce Clearance Procedures (A) – procedures to determine that the access of a Workforce member to ePHI is appropriate will be implemented.
- 9.3.3 Termination Procedures (A) – procedures for terminating access to ePHI when the employment of a Workforce member ends will be implemented.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

9.3.1 Authorization and/or Supervision (A)

Only those Workforce members who require access to ePHI to perform appropriate activities on behalf of the Plan will be permitted to have access to such information.

The HIPAA Privacy Officer, Security Officer, or a designee, will determine which Individuals or classes of Individuals can access PHI and ePHI as part of their job functions, and identify the categories of PHI and ePHI to which these access rights apply. The HIPAA Privacy Officer, Security Officer, or a designee will review requests for non-Routine Disclosures on an individual basis, using set criteria.

The Plan maintains a listing of personnel who are authorized to access PHI and ePHI. The current listing is documented in Section 4.1 of these HIPAA policies (the HIPAA "firewall").

The need for a screening process will be based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes will be applied to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the Individual.

Workforce members who work with ePHI or in areas where it may reasonably be anticipated to be accessed will appropriately trained and supervised. Non-Workforces members and others who work in areas where ePHI may be inadvertently or incidentally viewed or accessed, will receive appropriate Training and instruction regarding such information.

9.3.2 Workforce Clearance Procedures (A)

The Plan performs Workforce clearance procedures in several ways:

(a) The City has implemented recruiting, screening and hiring policies, procedures and practices on a organizational basis; and
(b) Reference checks and other appropriate mechanisms are also utilized by the City.

9.3.3 Termination Procedures (A)

Upon termination of employment, access privileges to ePHI, the Plan's Information Systems and work areas where ePHI may reasonably be anticipated to be accessed will be terminated. Termination of privileges and access will be effected immediately upon termination of employment, or sooner if circumstances warrant (e.g., in the case of an employee being terminated for cause).

When access to ePHI is no longer needed for a Workforce member to perform his or her job, access privileges will be revoked or modified as needed. The listing of personnel who are authorized to access PHI and ePHI (maintained in Section 4.1 of these HIPAA policies) will be updated to reflect this change.

TOPIC: Information Access Management
SUBJECT: Ensuring that access to ePHI is authorized, established, maintained and modified based on the minimum amount necessary for a Workforce member to perform his or her job effectively

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan's policies and procedures only allow for authorized access to ePHI in a manner that is consistent with the requirements of the HIPAA Privacy Rule. Access to ePHI is therefore authorized, established, maintained and modified based on the minimum amount of information necessary for a Workforce member to perform his or her job effectively. These policies will include addressing the following HIPAA Implementation Specifications:

- 9.4.1 Access Authorization (A) – policies and procedures for granting access to ePHI, for example, through a Workstation, Transaction, program, process or other mechanism will be implemented.
- 9.4.2 Access Establishment and Modification (A) – policies and procedures, that based on the Plan's Access Authorization policies, establish, document, review, and/or modify a User's right of access to a Workstation, Transaction, program or process will be implemented.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

9.4.1 Access Authorization (A)

Access to ePHI is granted in a manner that is consistent with the Plan's determination of the minimum amount of information required by members of the Workforce to perform his or her job. The Plan's policy on the minimum Use of PHI (and ePHI) is documented in Section 6.1 of these HIPAA policies. This includes procedures and standard protocols to limit the Use and Disclosure of PHI/ePHI to the minimum information reasonably necessary to achieve the purpose of that type of Use or Disclosure.

The Plan has determined who needs to have access to PHI/ePHI and identified the categories of such information to which access is needed and conditions appropriate to such access. For every type of Routine and permissible Use or Disclosure of PHI, the Plan will consider the minimum information reasonably necessary to achieve the purpose of that type of Use or Disclosure and will make every effort to ensure consistency. What is reasonable to comply with this policy will vary based on the circumstances. The Plan will use discretion to determine what the Minimum Necessary in each situation is.

9.4.2 Access Establishment and Modification (A)

The Plan maintains documentation regarding authorized access privileges. Access is modified or revoked when a User's job function or access needs change. Reviews of access rights are conducted at regular intervals to ensure continued appropriateness of levels of access.

Access privileges are immediately revoked when a User is no longer employed by the City or whose job function no longer includes duties associated with the Plan. Special care is taken in deactivating access when employment is involuntarily terminated.

Further information on specific procedures for granting and modifying access to various systems, facilities, User accounts, and applications containing ePHI, as well as for reviewing systems and applications access reports can be obtained by contacting the Security Officer or the CIS Network Team.

TOPIC: Security Awareness and Training
SUBJECT: Security awareness and Training for members of the Workforce

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has implemented a Security awareness and Training program for all members of its Workforce, including management. Training on the Plan's HIPAA policies and procedures as will be conducted in an appropriate manner so as to enable the members of the Workforce to carry out their job function(s) within the Plan.

Training will be provided to each appropriate member of the Workforce on privacy, Confidentiality and Security requirements that are applicable to their work. Each new member of the Workforce will receive the Training within four (4) weeks after joining the Plan's Workforce.

When there is a material change in the privacy policies and/or procedures, each member of the Workforce whose function is affected by the change will be trained within four (4) weeks after the change becomes effective

These policies will include addressing the following HIPAA Implementation Specifications:

- 9.5.1 Security Reminders (A) – periodic Security updates will be implemented.
- 9.5.2 Protection from Malicious Software (A) – procedures for guarding against, detecting, and reporting Malicious Software will be implemented.
- 9.5.3 Log-in Monitoring (A) – procedures for monitoring log-in attempts and reporting discrepancies will be implemented.
- 9.5.4 Password Management (A) – procedures for creating, changing and safeguarding Passwords will be adopted.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

A Security Training program will be provided for all existing and new members of the Workforce regarding the Security and privacy of ePHI and the Plan's Information Systems.

The Security Officer (or his or her designee) will determine the method of Training and documented orientation program to train appropriate staff. This may include memos, e-mailed notices, self-learning packets, distribution of policies and procedures, presentation materials, or other methods. The information can be taught at departmental meetings, Training meetings, one-on-one Training or by self-teaching. The person responsible for the Training session will provide a listing of who has received the Training, the trainer, and date of Training and copies of information disseminated to the Security Officer.

On-going Training will be conducted within four (4) weeks whenever there is a material change to the HIPAA Security requirements or to the Plan's policies and procedures. The delivery method for such on-going Training may vary and/or be revised as the circumstances allow. New employees entering into roles/functions within the firewall will be logged in and trained within four (4) weeks from the date they begin working with PHI as part of their designated job function.

The Plan will document its Training in written or electronic form and maintain such documentation for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

9.5.1 Security Reminders (A)

Periodic security reminders are distributed to each Workforce member and are viewable whenever a Workforce member logs on to the City's computer network system.

The CIS Network Team, in its discretion, may also distribute additional security reminders, security tips, and/or other timely information around IT and systems security at the City via e-mail or other method.

9.5.2 Protection from Malicious Software (A)

All Workstations and servers associated with Workforce members and ePHI include anti-virus software with current virus definition files installed and programmed to conduct automatic virus scanning. Security updates and patches for computer operating systems and software are installed as needed to reduce known vulnerabilities.

When a virus is suspected or detected, the Security Officer (or his or her designee) should be notified as soon as possible. Workforce members are not allowed to proceed with virus eradication efforts without appropriate authorization and/or supervision from the CIS Network Team. The infected machine, along with any other machines that may have been contaminated must be isolated from the network, scanned and repaired by the appropriate CIS personnel.

Information on virus and Malicious Software protection is included in the Plan's Security Training program. Workforce members are instructed not to download software from the Internet or install software on desktops or laptops without prior authorization.

Workforce members are instructed not to open e-mail attachments from unknown or untrustworthy sources. All e-mail attachments are scanned for the presence of viruses.

9.5.3 Log-in Monitoring (A)

Log-in attempts are monitored and tracked by the City's Information Systems. If an Individual attempts to log into the system using an incorrect Username or Password three (3) times, the User account will be automatically locked out and will be required to be reset by a CIS technician.

Further information on specific procedures for log-in monitoring, tracking, detection, identification, and/or Authorization violations (such as failed attempts to access systems, networks, or information) can be obtained by contacting the Security Officer or the CIS Network Team.

Documentation of log-in violations will be retained according to the City's record retention guidelines.

9.5.4 Password Management (A)

Members of the Workforce must follow the City's established guidelines for creating, changing and safeguarding Passwords:

Creating Passwords:

(a) Workforce members must create unique Passwords for each network User account, e-mail account and for screensaver protection;
(b) Passwords must contain at least eight (8) characters and should incorporate a mix of alpha and numeric characters;
(c) Passwords should not be words that are found in a dictionary; and
(d) Passwords should be easy to remember, but should not be based on personal information, such as family names, pet names, birth dates or other information that may be easily guessed.

Changing Passwords:

(a) Workforce members are required to change Passwords consistent with the City's standards, provided however, that such change must be done at least once every ninety (90) days; and
(b) Any previously used Password may not be reused for ten (10) generations of Passwords.

Safeguarding Passwords:

(a) Workforce members should not write down their Passwords and post them in a visible location or close to their Workstation;
(b) Passwords should not be stored in a public area; and
(c) Passwords should not to be shared with other Individuals – including co-workers, assistants, or systems administrators;

TOPIC: Security Incident Procedures
SUBJECT: Policies and procedures to address Security Incidents

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan maintains policies and procedures which are reasonably designed to address and identify all Security Incidents, including the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with systems operations in an Information System. These policies will include the following HIPAA Implementation Specification:

9.6.1 Response and Reporting – the Plan will identify and respond to suspected or known Security Incidents; mitigate, to the extent practicable, harmful effects of known Security Incidents; and document Security Incidents and their outcomes.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

9.6.1 Response and Reporting

Workforce members are trained to report suspected or actual Security Incidents dealing with unauthorized access, Use, Disclosure, modification, or destruction of ePHI to the Security Officer as soon as practicable. This includes incidents such as denial of service attacks, malicious code, viruses and worms.

Specific procedures for the operation, monitoring, and logging of the City's overall intrusion detection system, including virus and malicious code attacks, can be found by contacting the CIS Network Team.

All known Security Incidents will be investigated and documented by CIS. An appropriate response to a Security Incident will be determined based on the nature and severity of the Security Incident. Responses may include, but are not be limited to:

(a) the application of sanction against responsible personnel;
(b) the initiation of (additional) Security reminders;
(c) additional and/or updated Training on Security practices; and
(d) an evaluation of the adequacy of the Plan's existing Security measures.

Any harm resulting from a Security Incident will be mitigated to the extent practicable.

All known Security Incidents, together with the results of associated investigations will be documented by CIS and the results maintained according to the City's record retention guidelines.

Security Incidents involving an improper Disclosure of ePHI will be logged by the Security Official or a designee and maintained in conjunction with Sec. 8.2 of these HIPAA policies for a period of not less than six (6) years.

TOPIC: Contingency Plan
SUBJECT: Policies and procedures for responding to Information Systems emergencies

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will establish, and implement as necessary, policies and procedures for responding to emergencies and other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damage systems containing ePHI. Such policies and/or business continuity plans are required for all critical business functions of the Plan. These policies will establish the elements involved with business resumption in the event of a disaster and will include addressing the following HIPAA Implementation Specifications:

- 9.7.1 Data Backup Plan – procedures to create and maintain exact, retrievable copies of ePHI will be established and implemented.
- 9.7.2 Disaster Recovery Plan – procedures to restore any loss of data will be established.
- 9.7.3 Emergency Mode Operation Plan – procedures to enable continuation of critical business processes for the protection of the Security of ePHI while operating in emergency mode will be established (and implemented as needed).
- 9.7.4 Testing and Revision Procedures (A) – procedures for periodic testing and revision of contingency plans will be implemented.
- 9.7.5 Applications and Data Criticality Analysis (A) – the relative criticality of specific applications and data in support of other contingency plan components will be assessed.

The Security Officer will provide support and direction for the implementation of the contingency plan as it may relate to ePHI.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

9.7.1 Data Backup Plan

Procedures have been adopted by the City on an overall basis which allow the Plan to retrieve and/or restore exact copies of data, including ePHI. These procedures include the following and can be obtained by contacting the CIS Network Team.

(a) All databases are backed-up on a daily basis,
(b) A nightly incremental data backup is conducted, and
(c) Backup data is stored weekly off-site at a secure third-party location.

Where the Plan has not created the ePHI or does not otherwise maintain original ePHI, the data backup procedures may include recovering any lost or corrupted data from its original source, including but not limited to the Individual to whom the ePHI pertains.

9.7.2 Disaster Recovery Plan

Procedures have been established to allow for the restoration of any loss of data and/or ePHI. These procedures include continuous testing of the disaster recovery plan and can be obtained by contacting the CIS Network Team.

9.7.3 Emergency Mode Operation Plan

Procedures have been established to allow the continuation of the Plan's critical business processes and to protect ePHI while operating in emergency mode. These procedures can be obtained by contacting the CIS Network Team.

9.7.4 Testing and Revision Procedures (A)

The City conducts regular testing on its disaster recovery plan. Regular testing is conducted semi-annually (twice per year); additional ad hoc testing may be conducted on an as needed basis. The CIS Network Team is responsible for testing the contingency plan. Further information on testing and revision procedures can be obtained by contacting the CIS Network Team.

9.7.5 Applications and Data Criticality Analysis (A)

The relative criticality of the City's applications and data has been reviewed as part of the City's overall emergency planning process. The City has established guidance and plans for recovery tiers and the priority for restoration of services and data. Further information on the relative criticality of various applications and data can be obtained by contacting the CIS Network Team.

TOPIC: Evaluation
SUBJECT: Evaluating safeguards under the Security Rule and performing periodic technical and non-technical evaluations

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will evaluate its safeguards under the Security Rule and perform periodic technical and non-technical evaluations, based initially upon the standards implemented under the Security Rule, and subsequently in response to environmental or operational changes affecting the Security of ePHI, to establish the extent to which its policies and procedures meet the Security Rule's requirements.

PROCEDURES:

The Security Officer will coordinate the resources necessary to periodically evaluate the Plan's compliance with the Security Rule, as well as the overall Security environment of the Plan and its ePHI.

Evaluations will be conducted whenever there are changes affecting the ePHI created, received, maintained or transmitted by the Plan, provided however that a periodic evaluation will be conducted at least once every three (3) years.

Additional, ad hoc evaluations of the technical and non-technical components of the Plan's Security environment and its compliance with the requirements of the HIPAA Security Rule may be conducted as deemed necessary and appropriate to ensure the adequacy of Security measures and compliance with the Security Rule by the Security Officer.

Documentation of known Security Incidents may be reviewed periodically and included in the decision of whether to conduct an ad hoc evaluation.

The results of the any evaluations will be documented and retained for a period of at least six (6) years from the date the evaluation was conducted.

TOPIC: Facility Access Controls
SUBJECT: Limiting physical access to the Plan's electronic Information Systems and Facilities

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has implemented and maintains policies and procedures regarding Facility access controls to limit physical access to the company's facilities, work areas and electronic Information Systems, while ensuring that properly authorized access is allowed. These policies will include addressing the following HIPAA Implementation Specifications:

10.1.1 Contingency Operations (A) – procedures to allow Facility access in support of restoration of lost data under the disaster recovery plan and emergency operation plan in the event of an emergency will be established and implemented as necessary.

10.1.2 Facility Security Plan (A) – policies and procedures to safeguard the Facility and the equipment therein from unauthorized physical access, tampering and theft will be implemented.

10.1.3 Access Control and Validation Procedures (A) – procedures to control and validate a person's access to facilities based upon their role or function, including visitor control, and control of access to software programs for testing and revision will be implemented.

10.1.4 Maintenance Records (A) – policies and procedures to document repairs and modifications to the physical components of a Facility which are related to Security (for example, hardware, walls, doors and locks) will be implemented.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

10.1.1 Contingency Operations (A)

Limited, temporary authorization to access electronic Information Systems is granted to repair personnel or technicians during emergencies for the purpose of restoring lost data or repairing damaged equipment.

Members of the Plan's Workforce may be restricted from accessing ePHI during emergencies until data and/or damaged equipment is restored or repaired.

10.1.2 Facility Security Plan (A)

The Plan has addressed overall physical Security measures to prevent unauthorized access to its Facilities and employee work areas and to prevent tampering with or the theft of its equipment. More information on these overall facility Security measures can be found by contacting the HIPAA Security Officer. (See also, Section 10.1.3 below).

10.1.3 Access Control and Validation Procedures (A)

Access to employees' work areas is controlled and validated through restricted access to the Personnel Department, Benefits Office. The Benefits Office is locked and secured at all times when not staffed.

Security guards, metal detectors and surveillance cameras are employed onsite at the City and County Building.

Visitors to the Benefits Office must be escorted as appropriate and, if working near or with ePHI, have appropriate authorization and/or supervision.

Access to servers and other electronic equipment requires an additional level of Security with access codes distributed on a limited basis.

10.1.4 Maintenance Records (A)

The Plan has determined that maintenance records are not generally required for the Security of ePHI as it may be used by the Plan in its day-to-day activities. Access to ePHI is restricted to those Workforce members who require it to perform their job functions and who are specifically trained on the requirements of the HIPAA Security regulations as well as the specific Security precautions which the City has implemented. Numerous other safeguards are also in place to protect ePHI as described in this Manual.

At the present time, due to the limited risk of inappropriate use or disclosure of ePHI, the Plan has determined that it will not adopt formal maintenance records policies or procedures. The alternate safeguards described in this manual have been determined to be reasonable and appropriate to mitigate the risk to the Plan's ePHI.

TOPIC: Workstation Use
SUBJECT: Specifying the proper functions, manner of use and physical attributes of Workstations

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical surroundings of a specific Workstation or class of Workstations that can access ePHI.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

Workforce members utilize plan sponsor owned and maintained Workstations in the course of normal business on behalf of the Plan. The functions that can be performed by Workforce members are determined by their role and based upon approved and authorized User access requests. Workstations are configured with the appropriate software and applications based upon these approved functions. Only software packages approved by the CIS Network Team may be installed on plan sponsor computing systems or Workstations. The use of unapproved software is prohibited, as is the use of file sharing software or any hardware or software tools that could be employed to evaluate or compromise Information Systems Security.

Workforce members will not use profanity, obscenities or derogatory remarks in electronic communications. E-communications usage will be consistent with the standards of ethical and polite conduct as outlined in the City's employee code of conduct policy. Websites and other areas containing sexually explicit, racist, violent, criminal or other offensive or inappropriate materials may not be accessed by Workforce members. Workforce members who receive unsolicited offensive materials from third parties will not respond to, forward or re-distribute such materials either internally or externally, unless it is to the CIS Network Team to assist in the investigation of a complaint. Such unsolicited materials should be deleted upon receipt.

Training is provided to members of the Workforce regarding acceptable uses of Workstations that contain or permit access to ePHI are provided to members of the Workforce. Additional Training may be provided on an as needed basis to ensure Workforce members understand all procedures for compliance.

TOPIC: Workstation Security
SUBJECT: Physical safeguards for all Workstations with access to ePHI to restrict access to authorized Users

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan will implement Physical Safeguards for all Workstations that access ePHI in order to restrict access to authorized Users.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

All persons or classes of persons whose Workstations contain or permit access to ePHI have been identified. The Plan has taken reasonable precautions to confirm that such Workstations are physically safeguarded in a manner that maximizes Security and prevents unauthorized access.

Workforce members are required to take reasonable steps to prevent unauthorized access of unattended Workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed.

Additional Training may be provided on an as needed basis to ensure Workforce members understand all procedures for compliance.

TOPIC: Device and Media Controls
SUBJECT: Management of the receipt, removal and movement of hardware and Electronic Media that contain ePHI

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has implemented policies to govern the receipt and removal of hardware and Electronic Media that contain ePHI into and out of its facilities, as well as the movement of these items within its facilities. These policies will include addressing the following HIPAA Implementation Specifications:

- 10.4.1 Disposal – policies and procedures to address the final disposition of ePHI and/or the hardware or Electronic Media on which it is stored will be implemented.
- 10.4.2 Media Re-Use – procedures to remove ePHI from Electronic Media before the media are made available for re-Use will be established.
- 10.4.3 Accountability (A) – a record of the movements of hardware and Electronic Media and the person responsible for that record will be maintained.
- 10.4.4 Data Backup and Storage (A) – exact, retrievable copies of ePHI will be created, when needed, prior to the movement of equipment.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

Within the Plan, ePHI may be stored or maintained on hardware and Electronic Media such as storage devices (servers and shared or hard disk drives), desktop Workstations, diskettes, and CDs.

10.4.1 Disposal

Any ePHI that is stored on the hard drives of computers or other Electronic Media is removed and permanently erased through the use of a utility program to reformat all storage volumes and permanently remove all data before the disposal of the hardware or Electronic Media.

The City's off-site, third-party secure storage vendor will return or destroy any Electronic Media in storage prior to disposal, as may be requested by the Plan.

10.4.2 Media Re-Use

Any ePHI that is stored on the hard drives of computers or other Electronic Media is removed and permanently erased through the use of a utility program to reformat all storage volumes and permanently remove all data before the re-use of the hardware or Electronic Media.

10.4.3 Accountability (A)

The City maintains records documenting the physical movement of all hardware and electronic media into and out of the facility. Theses records are maintained by the CIS Network Team. Records on all assigned Workstations, laptops, and temporary Workstations ("Loaners") are also maintained (where applicable).

10.4.4 Data Backup and Storage (A)

An exact, retrievable copy of ePHI is created before any data migration or other major physical move of equipment that may result in damage or the loss of data. More information regarding such records can be obtained by contacting the HIPAA Security Officer or the CIS Network Team.

TOPIC: Access Control
SUBJECT: Technical Security measures for the Plan's electronic Information Systems

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

Technical Security measures, policies and procedures have been implemented for electronic Information Systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. These policies will include addressing the following HIPAA Implementation Specifications:

- 11.1.1 Unique User Identification – a unique name and/or number for identifying and tracking User identity will be assigned.
- 11.1.2 Emergency Access Procedure – procedures for obtaining necessary ePHI during an emergency will be established and implemented as necessary.
- 11.1.3 Automatic Logoff (A) – electronic procedures that terminate an electronic session after a predetermined period of inactivity will be implemented.
- 11.1.4 Encryption and Decryption (A) – a mechanism to encrypt and decrypt ePHI will be implemented.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

11.1.1 Unique User Identification

All Workforce members are assigned unique User Identification names or numbers that enable the Plan's Information System to identify, authenticate and track User identity.

Access control lists containing the records of such unique User IDs are updated promptly when access privileges are terminated or changed.

11.1.2 Emergency Access Procedure

Temporary access to the Plan's Information Systems and/or ePHI is provided in the event of emergencies. If emergency access is needed, a new User will be issued a User ID with a specific expiration date.

11.1.3 Automatic Logoff (A)

The Plan has determined that the following automatic logoff/lock-out procedures are sufficient to meet its Security needs:

(a) Workforce members with access to ePHI are required to utilize locking devices on their workstations (e.g. a password protected screensaver);
(b) Workstation locking should be enabled after ten (10) minutes of inactivity; and
(c) Workstation locking mechanisms should include the use of a unique user password.

11.1.4 Encryption and Decryption (A)

When possible, the Plan may encrypt stored data that is classified as confidential, including ePHI data stored on its servers and Workstations. Encryption technology should be installed and utilized to encrypt the hard disk drives of all laptop Workstations containing ePHI.

Specific details on the procedures for encrypting confidential information, including ePHI, are maintained by the CIS Network Team.

TOPIC: Audit Controls
SUBJECT: Recording and examining activity in Information Systems that contain or use ePHI

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT

The Plan will implement hardware, software, and/or procedural mechanisms that record and examine activity in Information Systems that contain or use ePHI.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES

The Plan is required to implement mechanisms that record and examine activity in Information Systems that contain or Use ePHI. The City or the Plan maintains the following audit controls:

(a) Event logs (incl. date and time-stamping of data changes);
(b) Security Incident tracking logs (incl. flagging of unauthorized attempts to access data); and/or
(c) Other internal Security controls and monitoring tools.

Changes to, or activities altering ePHI in systems or applications (such as creates, reads, updates or deletes) may be reviewed or tracked by the CIS Network Team. Such activity records may consist of any of the following elements:

(a) The type of activity performed;
(b) The date and time or access or alteration;
(c) The unique User ID of the person performing the activity; and/or
(d) The identifier of the record being accessed or altered.

Activities that alter applications containing ePHI are tracked using one or more of the above audit controls. Additional change management procedures may be utilized when necessary.

TOPIC: Integrity
SUBJECT: Protecting ePHI from improper alteration or destruction

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT

All ePHI maintained in the Plan's Information Systems is protected from improper alteration or destruction. The Plan has considered the risk and potential for improper alteration or destruction of ePHI maintained in its systems and has determined that the policies and procedures set forth herein are reasonable and sufficient to ensure the Integrity of the ePHI. These policies will include addressing the following HIPAA Implementation Specification:

11.3.1 Mechanism to Authenticate ePHI (A) – electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner will be implemented.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES

All approved Users with the ability to alter or destroy data have been identified as have been scenarios that may result in modification to ePHI data by unauthorized sources (e.g., hackers, disgruntled employees).

11.3.1 Mechanism to Authenticate ePHI (A)

The Plan's policies to protect ePHI from improper alteration or destruction include the following:

(a) Limiting access to data containing ePHI;
(b) Time-stamping all data changes and maintaining them in Information Systems History; and
(c) Creating regular backups of all electronic data (specific information on the Data Backup Plan is documented in Section 9.7.1 of these HIPAA policies).

Further information can be obtained by contacting the HIPAA Security Officer or the CIS Network Team.

TOPIC: Person or Entity Authentication
SUBJECT: Verifying that a person or entity seeking access to ePHI is the one claimed

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT:

The Plan has implemented reasonable procedures to verify that a person or entity seeking access to ePHI is the one claimed.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES:

Unique User IDs are assigned to all members of the Workforce. That User ID, in conjunction with an individually selected Password is required to logon to the Plan's Information Systems. An additional level of authentication in the form of a Smart Card ID is currently in the process of being implemented for access to the City's Information System.

Workforce members are required to follow the Plan's Password management policies and procedures to create and safeguard their User ID and Passwords to prevent unauthorized access to the Plan's Information System. (See, Section 9.5.4 of these HIPAA policies.)

Workforce members are strongly discouraged from sharing their logon ID or Password without prior approval of the Security Officer or the CIS Network Team.

Workforce members may not misrepresent themselves to the Plan's Information System by using another person's unique User ID.

TOPIC: Transmission Security
SUBJECT: Technical Security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communications network

EFFECTIVE DATE: April 20, 2005
REVISION DATE: November 30, 2009

POLICY STATEMENT

The Plan has implemented technical Security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. These policies will include addressing the following HIPAA Implementation Specifications:

11.5.1 Integrity Controls (A) –Security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of will be implemented.
11.5.2 Encryption (A) – a mechanism to encrypt ePHI whenever deemed appropriate will be implemented.

The Plan also specifically incorporates herein by reference those policies and procedures established and maintained by the City Information Systems ("CIS") Network Team, the City's supporting policies and standards, and any amendments or revisions thereto.

PROCEDURES

ePHI has been classified by the Plan as high risk information and should not be transmitted electronically unless reasonable methods have been taken to protect its Security. Only authorized Individuals may transmit ePHI. If ePHI is transmitted via e-mail communications, only the minimum amount of PHI needed to achieve the purpose of the communication is allowed to be transmitted. This should be determined in accordance with the Plan's minimum use of PHI policy contained in Section 6.1 of these HIPAA policies.

Methods of enabling secure transmissions and data Integrity during transmission include the use of secure servers and vendor transmission protocols (e.g., FTP and HTTPS) where available.

Additionally, if ePHI is transmitted via e-mail communications, the following Statement (or a functional equivalent) should be included:

> "This e-mail message, including any attachment(s), is for the sole use of the intended recipient(s) and may contain confidential information. Any unauthorized review, use, disclosure or distribution is strictly prohibited. If you are not the intended recipient, please immediately contact the sender by e-mail and delete this message."

11.5.1 Integrity Controls (A)

Methods of enabling secure transmissions and data Integrity during transmission include the use of secure servers and vendor transmission protocols (e.g., FTPS and HTTPS) where available.

Workforce members should limit the exchange of ePHI via e-mail. Archival storage of e-mails containing ePHI is permissible, but such e-mails should be sent to a secured location. E-mails containing ePHI should be deleted following the disposition of the issues to which they relate. If, however, the information must be retained beyond the disposition of the issue(s), the information should be stored in secured folders with limited access.

The Security Officer may also authorize or mandate the use of further integrity controls on an as needed basis as may be appropriate given the nature of the information and the potential risks posed.

11.5.2 Encryption (A)

Encryption (or a similarly secure method) should be utilized by Workforce members for the transmission of any data containing ePHI. An Encryption method should be coordinated with the recipient of any e-mail communications containing PHI.

Encryption technology is currently available for use by the Plan for securing transmissions in the following circumstances:

(a) Internal e-mails containing ePHI should be automatically encrypted by the sender through the City's internal Microsoft Outlook e-mail software; and

(b) Certain, pre-established vendor account representatives may be contacted in advance to set-up and coordinate external encryption options. The CIS Network Team may assist with coordination of any technical requirements as necessary.

The Security Officer may also authorize or mandate the use of encryption on an as needed basis as may be appropriate given the nature of the information and the potential risks posed.

TOPIC: Breach of Unsecured PHI
SUBJECT: Notification to Individuals, the media and the Secretary

EFFECTIVE DATE: September 23, 2009
REVISION DATE: November 30, 2009

POLICY STATEMENT

The Plan has established policies and procedures to provide notification following the discovery of a Breach of Unsecured PHI to, as applicable, affected Individuals, the media and the Secretary.

Notification to Individuals. The Plan will, following the discovery of a Breach, notify each Individual whose Unsecured PHI has been, or is reasonably believed by the Plan to have been accessed, acquired, used or disclosed as a result of such Breach.

Notification to the Media. For a breach of Unsecured PHI involving more than 500 residents of a State or jurisdiction, the Plan will, following discovery of the Breach, notify prominent media outlets serving the State or jurisdiction.

Notification to the Secretary. The Plan will, following the discovery of a Breach of Unsecured PHI, notify the Secretary.

Discovery of Breach. A Breach will be treated as discovered by the Plan as of the first day on which such Breach is known to the Plan, or, by exercising reasonable diligence would have been known to the Plan. The Plan will be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a Workforce member or agent of the Plan (determined in accordance with the federal common law of agency).

Risk Assessment. Following discovery of a potential Breach, the Plan will begin an investigation, conduct a risk assessment and, based on the results of the risk assessment, begin the applicable notification process.

Administrative Requirements. The Plan will comply with the administrative requirements applicable to this policy for Breach of Unsecured PHI with respect to: Training, Individuals' complaints to the Plan, Sanctions against Workforce members who fail to comply with the Plan's Breach of Unsecured PHI policies, refraining from intimidating or retaliatory acts, waiver of rights implementation of policies and procedures, and changes to the Plan's policies and procedures.

PROCEDURES

I. Breach Investigation

The Plan will name an individual to act as the investigator of the Breach (*e.g.*, privacy officer, security officer). The investigator will be responsible for the management of the Breach investigation, completion of a risk assessment, and coordinating with others, as appropriate. All documentation related to the Breach investigation, including the risk assessment, will be retained for a minimum of six (6) years.

II. Risk Assessment

To determine if an impermissible use or disclosure of PHI constitutes a Breach and requires notification to an affected Individual or the Secretary, the Plan will perform a risk assessment to determine if there is significant risk of harm to the Individual as a result of the impermissible Use or Disclosure. The Plan will document the risk assessment noting the outcome of the risk assessment process. The Plan has the burden of proof for demonstrating that the required notification to the affected Individual or the Secretary was made or that the Use or Disclosure did not constitute a Breach. In performing the risk assessment, the assessment will be fact specific and the Plan will consider a number of or combination of factors, such as: (1) consideration of who impermissibly used or to whom the information was impermissibly disclosed; (2) the type and amount of PHI involved; and (3) the potential for significant risk of financial, reputational, or other harm.

III. Notification

Notification to Individuals.
The Plan will provide the notification to an Individual whose Unsecured PHI has been the subject of a Breach without unreasonable delay and in no case later than sixty (60) days after discovery of a Breach.

Content of Notification. The notification will include, to the extent possible:

- A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
- A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
- A brief description of what the Plan is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and
- Contact procedures for Individuals to ask questions or learn additional information, which will include a toll-free telephone, an email address, Web site, or postal address.

The notification will be written in plain language.

Method of Notification. The notification will be provided in the following form:

Written notice. The Plan will provide written notification by first-class mail to the Individual at the last known address of the Individual or, if the Individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. If the Plan knows the Individual is deceased and has the address of the next of kin or personal representative of the Individual, the Plan will provide the written notification by first-class mail to either the next of kin or personal representative of the Individual. The notification may be provided in one ore more mailings as information is available.

Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the Individual as described above, a substitute form of notice reasonably calculated to reach the Individual will be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the Individual.

- In the case in which there is insufficient or out-of-date contact information for fewer than ten (10) Individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.
- In the case in which there is insufficient or out-of-date contact information for ten (10) or more Individuals, then such substitute notice will:
- Be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of the Web site of the Plan, or conspicuous notice in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely reside; and
- Include a toll-free phone number that remains active for at least ninety (90) days where an Individual can learn whether the Individual's Unsecured PHI may be included in the Breach.

Additional Notice in Urgent Situations. In any case deemed by the Plan to require urgency because of possible imminent misuse of Unsecured PHI, the Plan may provide information to Individuals by telephone or other means, as appropriate, in addition to the notices described above.

Notification to the Media.
For a Breach of Unsecured PHI involving more than 500 residents of a State or jurisdiction, the Plan will, upon discovery of the Breach, notify prominent media outlets serving the State or jurisdiction. The Plan will provide the notification without unreasonable delay and in no case later than sixty (60) days after discovery of the Breach. The content of the notification to the media will meet the requirements described above for Notification to Individuals.

Notification to the Secretary.
The Plan will, following the discovery of a Breach of Unsecured PHI, notify the Secretary. For Breaches of Unsecured PHI involving 500 or more Individuals, a Plan will, subject to the exception noted below, provide this notification contemporaneously with the notice required to Individuals and in the manner specified on the HHS Web site.

> Exception. If a Law Enforcement Official states to the Plan that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Plan will: (a) if the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) if the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

IV. Maintenance of Breach Log

For Breaches of Unsecured PHI involving less than 500 Individuals, the Plan will maintain a log or other documentation of such Breaches and, not later than sixty (60) days after the end of each calendar year, provide this notification for Breaches occurring during the preceding calendar year, in the manner specified on the HHS Web Site.

The Plan will maintain a process to record or log all breaches of Unsecured PHI. The following information will be logged for each Breach:

(1) A description of what happened, including the date of the Breach, the date of the discovery of the Breach, and the number of Individuals affected, if known.

(2) A description of the types of Unsecured PHI that were involved in the Breach (*e.g.*, full name, Social Security number, date of birth, account number, home address).

(3) A description of the action taken with regard to notification of the affected Individuals or the Secretary regarding the breach.

V. Administrative Requirements

The Plan will apply the same policies applicable to the Privacy Rule to this policy for Breach of Unsecured PHI with respect to: Training, Individuals' complaints to the Plan, Sanctions against Workforce members who fail to comply with the Plan's Breach of Unsecured PHI policies, refraining from intimidating or retaliatory acts, waiver of rights, implementation of policies and procedures, and changes to the Plan's policies and procedures.

TOPIC: Definitions of HIPAA Terms
SUBJECT: HIPAA Terms and Definitions

EFFECTIVE DATE: April 14, 2003
REVISION DATE: November 30, 2009

Access – The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "Access" as used in regard to the HIPAA Security Rule, but not the HIPAA Privacy Rule.)

Administrative Safeguards – Administrative actions, and the policies and procedures, to manage the selection, development, implementation, and maintenance of Security measures to protect ePHI and to manage the conduct of the Covered Entity's Workforce in relation to the protection of that information.

Authentication – The corroboration that a person is the one claimed.

Authorization - The mechanism for obtaining permission for the Use and/or Disclosure of Health Information at any time other than at time of enrollment.

Availability – The property that data or information is accessible and Useable upon demand by an authorized person.

Breach - The acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the Security or Privacy of the PHI. For purposes of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the Individual to whom the PHI pertains. A Use or Disclosure of PHI that does not include the identifiers listed at § 45 CFR 164.514(e)(2) (Limited Data Set), date of birth, and zip code does not compromise the Security or Privacy of the PHI.

Breach excludes:

- Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of a Covered Entity or Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under the Privacy Rule.
- Any inadvertent Disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or Organized Health Care Arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

- A Disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

Business Associate - A(n) person / entity outside the Workforce of the Covered Entity who performs or assists in the performance of a function or activity involving the Use or Disclosure of Individually Identifiable Health Information or any other regulated function or activity, including but not limited, to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business associate may also provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates. The provision of the service involves the Disclosure of Individually Identifiable Health Information from (a) the Covered Entity, (b) the Organized Health Care Arrangement, or (c) from another Business Associate of the Covered Entity or Organized Health Care Arrangement, to the person / entity.

A Covered Entity participating in an Organized Health Care Arrangement can become a Business Associate to the Organized Health Care Arrangement by providing the activities as described above. The Covered Entity does not become a Business Associate of other covered entities participating in the Organized Health Care Arrangement.

A Covered Entity may be a Business Associate of another Covered Entity.

CMS - The Centers for Medicare and Medicaid Services within the Department of Health and Human Services.

Confidentiality - The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity - A Health Plan, a Health Care Clearinghouse, or a Health Care Provider who transmits any Health Information in electronic form in connection with a standard or covered Transaction.

Covered Functions - Those functions of a Covered Entity the performance of which makes the entity a Health Plan, Health Care Provider, or Health Care Clearinghouse.

De-Identification of Information - Information from which the following identifiers have been removed or concealed:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to their current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, or the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an Individual including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older:
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical Record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images, and
- Any other unique identifying number, characteristic, or code that the Covered Entity has reason to believe may be available to an anticipated recipient of information.

Designated Record Set - A group of Records maintained by or for a Group Health Plan, consisting of enrollment, Payment, claims adjudication, and case or medical management record systems; or Used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. The Designated Record Set will include only PHI that was created or received beginning on or after April 14, 2004. Please also refer to the definition of "Record".

Disclosure - The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic Media - Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media Used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via Electronic Media, because the information being exchanged did not exist in electronic form before the Transaction.

Electronic Protected Health Information (ePHI) - Protected Health Information that is transmitted by or maintained in Electronic Media.

Encryption – The Use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without Use of a confidential process or key, and where such process or key has not been breached.

Facility – The physical premises and the interior and exterior of a building(s).

Family Member – With respect to an Individual, a Family Member is: (1) A dependent of the Individual; or (2) Any person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the Individual or of a dependent of the Individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

First-degree relatives include parents, spouses, siblings, and children. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins. Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Genetic Information –

(1) Subject to paragraphs (2) and (3) below, Genetic Information means, with respect to any Individual, information about: (i) Such Individual's Genetic Tests; (ii) The Genetic Tests of Family Members of such Individual; (iii) The Manifestation of a disease or disorder in Family Members of such Individual; or (iv) Any request for, or receipt of, Genetic Services, or participation in clinical research which includes Genetic Services, by such Individual or any Family Member of such Individual.

(2) Any reference in this Manual to Genetic Information concerning an Individual or Family Member of an Individual will include the Genetic Information of: (i) A fetus carried by the Individual or Family Member who is a pregnant woman; and (ii) Any embryo legally held by an Individual or Family Member utilizing an assisted reproductive technology.

(3) Genetic Information excludes information about the sex or age of any Individual.

Genetic Services – Genetic Services means: (1) A Genetic Test; (2) Genetic Counseling (including obtaining, interpreting, or assessing Genetic Information); or Genetic education.

Genetic Test – Genetic Test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic Test does not include an analysis of proteins or metabolites that is directly related to a Manifested disease, disorder, or pathological condition.

Group Health Plan - An employee welfare benefit plan (as defined in the Employee Retirement Income and Security Act of 1974), including insured and self insured plans, to the extent that the Plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

- Has 50 or more Individuals, or
- Is administered by an entity other than the employer that established and maintains the plan(s).

HHS - The Department of Health and Human Services.

HIPAA – The Health Insurance Portability and Accountability Act of 1996, and any regulations promulgated thereunder, as may be amended and in effect from time to time.

Health Care - The provision of care, services, or supplies to a patient includes any:

- preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body; and/or
- sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription.

Health Care Clearinghouse - A public or private entity that conducts either of the following:

- Processes or facilitates the processing of Health Information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard Transaction; or
- Receives a standard Transaction from another entity and processes or facilitates the processing of Health Information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations - Any of the following activities of the Covered Entity to the extent that the activities are related to Covered Functions:

- Conducting quality assessment and improvement activities, including evaluating outcomes, and developing clinical guidelines;
- Reviewing the competence or qualifications of Health Care professionals, evaluating practitioner and provider performance, Health Plan performance, conducting Training programs in which undergraduate and graduate students and trainees in all areas of Health Care learn under supervision to practice as Health Care Providers (e.g., residency programs, grand rounds, nursing practicums), accreditation, certification, licensing or credentialing activities;
- Insurance rating and other insurance activities relating to the renewal of a contract for insurance, including underwriting, experience rating, and reinsurance, but only when the Individuals are already enrolled in the Health Plan conducting such activities and only when the Use or Disclosure of such Protected Health Information relates to an existing contract of insurance (including the renewal of such a contract);
- Conducting or arranging for medical review, legal services, auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of Payment or coverage policies; and
- Business management and general administrative activities of the entity, including, but not limited to:
    - Management activities relating to implementation of and compliance with HIPAA;
    - Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that Protected

Health Information is not disclosed to such policy holder, plan sponsor, or customer;
- Resolution of internal grievances;
- The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and
- Consistent with the applicable requirements of creating de-identified Health Information or a Limited Data Set, and fundraising for the benefit of the Covered Entity.

Health Care Provider - A provider of medical or health services and any other person or organization that furnishes, bills, or is paid for Health Care in the normal course of business.

Health Information - Any information, including Genetic 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 that relates to the past, present, or future physical or mental health or condition of an Individual, the provision of Health Care to an Individual, or the past, present, or future Payment for the provision of Health Care to an Individual.

Health Insurance Issuer - An insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State Law that regulates insurance. Such term does not include a Group Health Plan.

Health Maintenance Organization (HMO) - A federally qualified HMO, an organization recognized as an HMO under State Law, or a similar organization regulated for solvency under State Law in the same manner and to the same extent as such an HMO.

Health Plan - An Individual plan or Group Health Plan that provides, or pays the cost of medical care. A Health Plan includes the following, singly or in combination:

- A Group Health Plan;
- A Health Insurance Issuer;
- An HMO;
- Part A or Part B of the Medicare program;
- The Medicaid program;
- An issuer of a Medicare supplemental policy;
- An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy;
- An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers;
- The Health Care program for active military personnel;
- The veterans Health Care program;
- The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS);

- The Indian Health Service program under the Indian Health Care Improvement Act;
- The Federal Employees Health Benefits Program;
- An approved State child Health Plan, providing benefits for child health assistance;
- The Medicare + Choice program under Part C;
- A high risk pool that is a mechanism established under State Law to provide health insurance coverage or comparable coverage to eligible Individuals; and
- Any other Individual or group plan, or combination of Individual or group plans, that provides or pays for the cost of medical care.

A Health Plan excludes:

- Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits; and
- A government-funded program (other than one listed in the above paragraph of this definition) whose principal purpose is other than providing, or paying the cost of, Health Care; or whose principal activity is:
    - The direct provision of Health Care to persons; or
    - The making of grants to fund the direct provision of Health Care to persons.

Implementation Specification - Specific requirements or instructions for implementing a standard.

Incident Report Procedures - The documented formal mechanism employed to document Security Incidents.

Individual - The person who is the subject of Protected Health Information.

Individually Identifiable Health Information - Information that is a subset of Health Information, including demographic information collected from an Individual, and:

- 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 or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future Payment for the provision of Health Care to an Individual; and
- That identifies the Individual; or
- With respect to which there is a reasonable basis to believe the information can be Used to identify the Individual.

Individual Identifiers - Includes the following: name; address, including street address, city, county, zip code, and equivalent geocodes; names of relatives; name of employers; birth date; telephone numbers; fax numbers; electronic mail addresses; social Security number; medical Record number; Health Plan beneficiary number; account number; certificate/license number; any vehicle or other device serial number; web universal resource locator (URL); internet protocol (IP) address number; finger or voice prints; photographic images; and any other unique identifying number, characteristic, or code that the Covered Entity has reason to believe may be available to an anticipated recipient of the information.

Information System – An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity – The property that data or information have not been altered or destroyed in an unauthorized manner.

Law Enforcement Official - An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- Investigate or conduct an official inquiry into a potential violation of law; or
- Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set - Protected Health Information that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:

- Names;
- Postal address information, other than town or city, State, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical Record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

Malicious Software – Software, for example, a virus, designed to damage or disrupt a system.

Manifestation or Manifested – Manifestation or manifested means, with respect to a disease, disorder, or pathological condition, that an Individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a Health Care professional with appropriate training and expertise in the field of medicine involved. For purposes of this definition, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on Genetic Information.

Minimum Necessary - The minimum amount of Health Information necessary to accomplish the intended purpose of the Use or Disclosure is Used or disclosed except in the following situations:

- Disclosures or requests by a health provider for Treatment;
- When an Individual requests the Health Plan, Health Care Provider, or other Covered Entity to Use or disclose his/her information under the Authorization procedure;
- When the Individual requests access to his/her own Protected Health Information in Designated Record Sets;
- When the Secretary requests access to the information to ensure compliance or investigate a complaint;
- When Required by Law or permitted (the instances set forth above in the section on permissible Disclosures); and
- When the information is made by a Health Care Provider to the Health Plan pursuant to a request for compliance audit and related purposes.

More Stringent - In the context of a comparison of a provision of State Law and a standard, requirement, or Implementation Specification, a State Law that meets one or more of the following criteria:

- With respect to a Use or Disclosure, the law prohibits or restricts a Use or Disclosure in circumstances under which such Use or Disclosure otherwise would be permitted, except if the Disclosure is:
    - Required by the Secretary in connection with determining whether a Covered Entity is in compliance with this subchapter; or
    - To the Individual who is the subject of the Individually Identifiable Health Information.
- With respect to the rights of an Individual, who is the subject of the Individually Identifiable Health Information regarding access to or amendment of Individually Identifiable Health Information, permits greater rights of access or amendment;
- With respect to information to be provided to an Individual who is the subject of the Individually Identifiable Health Information about a Use, a Disclosure, rights, and remedies, provides the greater amount of information;
- With respect to the form, substance, or the need for express legal permission from an Individual, who is the subject of the Individually Identifiable Health Information, for Use or Disclosure of Individually Identifiable Health Information, provides requirements that narrow the scope or duration, increase the privacy

protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission;
- With respect to recordkeeping or requirements relating to accounting of Disclosures, provides for the retention or reporting of more detailed information or for a longer duration; and
- With respect to any other matter, provides greater privacy protection for the Individual who is the subject of the Individually Identifiable Health Information.

Non-Routine Permissible Uses and Disclosures - Information disclosed for purposes other than Treatment, Payment and Health Care Operations. The following are included in the definition of permissible Disclosure of Protected Health Information: public health activities; mandatory abuse reporting; oversight activities; judicial or administrative activities; Law Enforcement Officials reporting; medical examiners reporting; organ donations; research activities; avert a serious threat activities; Treatment of special government related classes; workers compensation reporting; Secretary of the Department of Health and Human Services requests and as otherwise Required by Law.

Organized Health Care Arrangement – An Organized Health Care Arrangement includes any of the following:

- A clinically integrated care setting in which Individuals typically receive Health Care from more than one Health Care Provider;
- An organized system of Health Care in which more than one Covered Entity participates, and in which the participating covered entities:
    - Hold themselves out to the public as participating in a joint arrangement; and
    - Participate in joint activities that include at least one of the following:
        - Utilization review, in which Health Care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
        - Quality assessment and improvement activities, in which Treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
    - Payment activities, if the financial risk for delivering Health Care is shared, in part or in whole, by participating covered entities through the joint arrangement and if Protected Health Information created or received by a Covered Entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
- A Group Health Plan and a Health Insurance Issuer or HMO with respect to such Group Health Plan, but only with respect to Protected Health Information created or received by such Health Insurance Issuer or HMO that relates to Individuals who are or who have been Individuals or beneficiaries in such Group Health Plan;
- A Group Health Plan and one or more other Group Health Plans each of which are maintained by the same plan sponsor; or
- The Group Health Plans and Health Insurance Issuers or HMOs with respect to such Group Health Plans, but only with respect to Protected Health Information

created or received by such Health Insurance Issuers or HMOs that relates to Individuals who are or have been Individuals or beneficiaries in any of such Group Health Plans.

Password – Confidential Authentication information composed of a string of characters.

Payment - Activities undertaken by a Health Plan (or by a Business Associate on behalf of a Health Plan) to determine its responsibilities for coverage under the Health Plan policy or contract including the actual Payment under the policy or contract, or by a Health Care Provider (or by a Business Associate on behalf of a provider) to obtain reimbursement for the provision of Health Care. Payment activities include, but are not limited to:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining Payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related Health Care data processing;
- Review of Health Care services with respect to medical necessity, coverage under a Health Plan, appropriateness of care, or justification of charges;
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:
    - Name and address;
    - Date of birth;
    - Social Security number;
    - Payment history;
    - Account number; and
    - Name and address of the Health Care Provider and/or Health Plan.

Physical Safeguards – Physical measures, policies, and procedures to protect a Covered Entity's electronic Information Systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Plan – The Educational Testing Service Welfare Benefits Plan and/or the Educational Testing Service Group Cafeteria Plan. As used herein, the term Plan only refers to TIAA' HIPAA covered benefit programs.

Plan Administration Functions - The administration functions performed by the plan sponsor of a Group Health Plan on behalf of the Group Health Plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Privacy Officer – The HIPAA Privacy Officer (or Privacy Official) is the person responsible for the development and implementation of the Plan's privacy policies and procedures.

Protected Health Information (PHI) - Individually Identifiable Health Information that is transmitted by Electronic Media, maintained in any medium, or transmitted or maintained in any other form or medium, by a Covered Entity. PHI excludes Individually Identifiable Health Information in education records defined and covered by the Family Educational Right and Privacy Act for students in primary and secondary education and employment records held by a Covered Entity in its role as employer.

Providing an Accounting of Disclosures - Providing Individuals with an accounting of all Disclosures of their Protected Health Information, except for Disclosures for Treatment, Payment and Health Care Operations, Disclosures pursuant to a valid Authorization and certain Disclosures to health oversight or law enforcement agencies.

Providing Individuals Access to their Information and Records - Ensuring that Individuals have access to their own Protected Health Information including access to such information in a Business Associate's Designated Record Set that is not a duplicate of the information held by the provider or plan.

Providing for Amendment or Correction of Records - Implementing an Individual's right to request amendment or correction of the Individual's Protected Health Information.

Public Health Authority - An agency or authority of the United States, a State, a 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, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Reasonable Evidence of Identity - A written Statement from the government agency, on the agency's letterhead, that the person or entity is acting under the agency's authority; or other evidence or documentation, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person or entity is acting on behalf of or under the agency's authority.

Reasonable Evidence of Authority - A written Statement of the legal authority under which the information is requested (a request for Disclosure made by official legal process issued by a grand jury or a judicial or administrative body is presumed to constitute reasonable legal authority); or, where the request is made orally, an oral Statement of such authority.

Record - 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.

Relates to the Privacy of Individually Identifiable Health Information - With respect to a State Law, that the State Law has the specific purpose of protecting the privacy of Health Information or affects the privacy of Health Information in a direct, clear, and substantial way.

Requesting Restrictions on Uses and Disclosures - Individuals may exercise their right to inform their Health Care Provider of restrictions on the Uses or Disclosures of their Protected Health Information.

Required by Law - A mandate contained in law that compels an entity to make a Use or Disclosure of Protected Health Information and that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to Health Care Providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if Payment is sought under a government program providing public benefits.

Routine - Protected Health Information disclosed for the purpose of Treatment, Payment and Health Care Operations.

Sanctions - Sanctions against members of its Workforce who fail to comply with the Plan's policies and procedures on Protected Health Information or with the privacy or Security requirements in connection with Protected Health Information held by the Health Plan or its Business Associates.

Secretary - The Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Security (Security Measures) – Encompass all of the Administrative, Physical, and Technical Safeguards in an Information System.

Security Incident – The attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with systems operations in an Information System.

Security Officer – The HIPAA Security Officer (or Security Official) is the person responsible for the development and implementation of the Plan's HIPAA Security policies and procedures.

Standard - A prescribed set of rules, conditions, or requirements concerning classification of components, specification of materials, performance or operations, or delineation of procedures in describing products, systems, services, or practices, with respect to the privacy or Security of Individually Identifiable Health Information.

State - The 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

State Law - A constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

Summary Health Information - Information that may be Individually identifiable Health Information, and:

- That summarizes the claims history, claims expenses, or type of claims experienced by Individuals for whom a plan sponsor has provided health benefits under a Group Health Plan; and
- From which the information has been de-identified (see De-identification), except that the geographic information need only be aggregated to the level of a five-digit zip code.

Technical Safeguards – The technology and the policy and procedures for its use that protect ePHI and control access to it.

Training - Training persons in the Workforce who are likely to obtain access to Protected Health Information or electronic Protected Health Information on the Health Plan's policies and procedures, required under the HIPAA privacy and Security regulations, that is relevant to their activities.

Transaction - The transmission of information between two parties to carry out financial or administrative activities related to Health Care. A "Transaction" would mean any of the following:

- Health claims or equivalent encounter information. This Transaction could be used to submit Health Care claim billing information, encounter information, or both, from Health Care Providers to payers, either directly or via intermediary billers and claims clearinghouses;
- Health Care Payment and remittance advice. This Transaction could be used by a Health Plan to make a Payment to a financial institution for a Health Care Provider (sending Payment only), to send an explanation of benefits remittance advice directly to a Health Care Provider (sending data only), or to make Payment and send an explanation of benefits remittance advice to a health car provider via a financial institution (sending both Payment and data);
- Coordination of benefits. This Transaction could be used to transmit Health Care claims and billing Payment information between payers with different Payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the furnishing, billing, and/or Payment of Health Care services within a specific Health Care/insurance industry segment;
- Health claims status. This Transaction could be used by Health Care Providers and recipients of Health Care products or services (or their authorized agents) to request the status of a Health Care claim or encounter from a Health Plan;

- Enrollment and disenrollment in a Health Plan. This Transaction could be used to establish communication between the sponsor of a health benefit and the payer. It provides enrollment data, such as subscriber and dependents, employer information, and primary care Health Care Provider information. A sponsor would be the backer of the coverage, benefit, or product. A sponsor could be an employer, union, government agency, association, or insurance company. The Health Plan would refer to an entity that pays claims, administers the insurance product or benefit, or both;
- Eligibility for a Health Plan. This Transaction could be used to inquire about the eligibility, coverage, or benefits associated with a benefit plan, employer, plan sponsor, subscriber, or a dependent under the subscriber's policy. It also could be Used to communicate information about or changes to eligibility, coverage, or benefits from information sources (such as insurers, sponsors, and payers) to information receivers (such as physicians, hospitals, third party administrators, and government agencies);
- Health Plan premium Payments. This Transaction could be used by, for example, employers, employees, unions, and associations to make and keep track of Payments of Health Plan premiums to their health insurers. This Transaction could also be Used by a Health Care Provider, acting as liaison for the beneficiary, to make Payment to a health insurer for coinsurance, co-Payments, and deductibles;
- Referral certification and Authorization. This Transaction could be used to transmit Health Care service referral information between Health Care Providers, Health Care Providers furnishing services, and payers. It could also be Used to obtain Authorization for certain Health Care services from a Health Plan;
- First report of injury. This Transaction could be Used to report information pertaining to an injury, illness, or incident to entities interested in the information for statistical, legal, claims, and risk management processing requirements;
- Health claims attachments. This Transaction could be Used to transmit Health Care service information, such as subscriber, patient, demographic, diagnosis, or Treatment data for the purpose of a request for review, certification, notification, or reporting the outcome of a Health Care services review; and
- Other Transactions as the Secretary may prescribe by regulation. The Secretary may adopt Standards, and data elements for those Standards, for other financial and administrative Transactions deemed appropriate by the Secretary. These Transactions would be consistent with the goals of improving the operation of the Health Care system and reducing administrative costs.

Treatment - The provision, coordination, or management of Health Care and related services by one or more Health Care Providers, including the coordination or management of Health Care by a Health Care Provider with a third party; consultation between Health Care Providers relating to a patient; or the referral of a patient for Health Care from one Health Care Provider to another.

Underwriting Purposes –
(1) Except as provided in the second paragraph of this definition, Underwriting Purposes means:

i. Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the Plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
ii. The computation of premium or contribution amounts under the Plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program;
iii. The application of any pre-existing condition exclusion under the Plan, coverage, or policy; and
iv. Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(2) Underwriting Purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the Plan, coverage or policy.

Unsecured PHI - PHI that is not rendered unusable, unreadable, or indecipherable to authorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under Section 13402(h)(2) of Pub.L.111-5 on the HHS website. Unsecured PHI includes information in any form or medium, including electronic, paper or oral form.

PHI is rendered unusable, unreadable, or indecipherable to authorized individuals if one or more of the following applies:

(1) Electronic PHI has been encrypted as specified in the Security Rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

a. Valid encryption processes for data at rest (*i.e.*, data that resides in databases, file systems, flash drives, memory, and any other structured storage systems) are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*

b. Valid encryption processes for data in motion (*i.e.*, data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange) are those which comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport*

Layer Security (TLS) Implementations; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standards FIPS) 140-2 validated.

(2) The media on which the PHI is stored or recorded have been destroyed in on of the following ways:

a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

b. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Use - The sharing, employment, application, utilization, examination or analysis of Individually Identifiable Health Information within an entity that holds the information.

User – A person or entity with authorized access.

Workforce - The employees, volunteers, trainees and other persons under the direct control of a Covered Entity, including persons providing labor on an unpaid basis.

Workstation – An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and Electronic Media stored in its immediate environment.

CITY OF PITTSBURGH

AUTHORIZATION FORM

The City of Pittsburgh Group Health Plan
Release Authorization Form
for HIPAA Protected Health Information (PHI)

Authorization expiration date or event:	**Member Name:** (Last, First)	
	Member ID:	
Person/entity authorized to release PHI:		**Person/entity authorized to receive PHI:**
Description of PHI authorized to be disclosed:		**Purpose of requested disclosure:**
If this authorization is not signed by the individual to whom the PHI pertains but is signed by a personal representative of the individual, please describe below such representative's authority to act on behalf of the individual:		
Member Signature and Date:		

Member rights:

Member signing this release form has the right to revoke this authorization in writing at any time, except during a contestability period or to the extent that action has already been taken in reliance on this signed authorization.

When information authorized to be released on this form is used or disclosed pursuant to this authorization, it may be subject to re-disclosure by the recipient and may no longer be protected by HIPAA regulations.

You may inspect or copy the information to be used or disclosed pursuant to this authorization. You may also refuse to sign this authorization.

The City of Pittsburgh Group Health Plan will not condition treatment, payment, enrollment or eligibility for benefits on whether you sign this authorization when the prohibition on conditioning of authorizations applies.

A copy of the signed authorization must be given to you.

Business Associate	Service Performed	Contract Status and Comments	Contact Information (Name, address, phone, e-mail)	Date Mailed	Date Completed
1. Employee Benefit Data Services (EBDS)	■ FSA and COBRA administration	■ BAA signed in 2003 ■ Needs to be updated			
2. Highmark BCBS	■ Medical	■ Insured vendor ■ Discloses personal information in some situations, however ■ Need to review contract language and determine if BAA-like provisions should be added			
3. Towers Perrin	■ H&W Consultant	■ BAA signed in 2003 ■ Needs to determine if PHI is needed from the Plan to perform consulting services			

THE CITY OF PITTSBURGH GROUP HEALTH PLAN MAINTAINS AN INVENTORY OF BUSINESS ASSOCIATE AGREEMENTS, AMENDMENTS, AND CERTIFICATIONS.

PLEASE CONTACT THE HIPAA PRIVACY OFFICER FOR COPIES OF THESE AGREEMENTS.

THE CITY OF PITTSBURGH GROUP HEALTH PLAN MAINTAINS A CURRENT NOTICE OF PRIVACY PRACTICES.

PLEASE CONTACT THE HIPAA PRIVACY OFFICER FOR COPIES OF THE CITY'S NOTICE OF PRIVACY PRACTICES.

The City of Pittsburgh Group Health Plan

Notice of Privacy Practices – Distribution Log

Version of Notice Provided (e.g., full, revised, reminder notice)	***Employee Group(s) Receiving Notice***	***Method of Distribution (e.g., electronic, mail, etc.)***	***Date of Distribution***
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

The City of Pittsburgh Group Health Plan

HIPAA Non-Routine Disclosures Log

Item #	*Individual / Subject of the PHI*	*Date*	*Specific PHI Disclosed*	*Purpose*	*Mode*	*Recipients to Whom PHI was Disclosed*
1.						
2.						
3.						
4.						
5.						
6.						

Notes:
(1) The Plan will log all Non-Routine Disclosures in writing
(2) Contents of log will be reviewed upon request by any Individual for an Accounting of Disclosures
(3) Non-Routine Disclosure log s will be forwarded to and reviewed by the Privacy Officer periodically

Appendix H

HIPAA Breach Notification Log

Incident #	*Date of Discovery*	*Date of Breach*	*Brief Description of Breach, including description of unsecured PHI and number of individuals affected, if known*	*Notification Date*	*Business Associate (if applicable)*	*Action(s) Taken*
1.						
2.						
3.						
4.						
5.						
6.						

The City of Pittsburgh Group Health Plan

HIPAA Privacy and Security Training Completion Form

I have received training on safeguarding protected health information under the Health Insurance Portability and Accountability Act (HIPAA) for The City of Pittsburgh Group Health Plan. I understand and agree to comply with the Plan's privacy and security policies and procedures that apply to my job.

Course Name: **Safeguarding PHI: HIPAA Privacy and Security Overview**

Date of Training: _____

Name (Please Print)	***Employee ID Number***	***Signature***	***Date***
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			