

## HIPAA POLICIES AND PROCEDURES

---

### I. Introduction

The City of Wyoming (“Employer”) sponsors one or more health plan(s) (the “Plan”). The Plan is a covered entity, as that term is defined under the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”). HIPAA restricts the ability of the Plan and Employer to use and disclose protected health information (“PHI”).

Protected Health Information (“PHI”). Protected health information (“PHI”) means individually identifiable health information that is maintained or transmitted by a covered entity (such as the Plan), subject to specific exclusions. For example, employment records held by a covered entity in its role as an employer is not PHI.

PHI is individually identifiable if it is created or received by a covered entity, relates to the past, present, or future physical or mental health or condition of an individual (such as a Plan participant), the provision of health care to such an individual, or the past, present, or future payment for the provision of health care to such an individual, and identifies such an individual, or there is a reasonable basis to believe the information can be used to identify the individual.

De-identified information is not individually identifiable health information and therefore, is not PHI. De-identified information is where the following identifiers are removed and the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information: Name, address, dates directly related to the individual’s receipt of health care treatment, telephone number, fax number, email address, Social Security number, medical record number, health plan beneficiary number, account number, certificate/license number, vehicle identifier and serial number including license plate number, device identifier and serial number, web universal resource locator (URL), intranet protocol (IP) address, biometric identifiers, full face photographic images and any other unique identifying number, characteristic or code.

PHI includes genetic information. An individual’s genetic information may not be used for underwriting purposes with respect to the Plan (except in the case of any long term care benefits).

## *HIPAA Policies And Procedures*

It is Employer's intent that the Plan comply fully with HIPAA's requirements. For this purpose, HIPAA's requirements include all amendments to HIPAA and regulations issued pursuant to HIPAA, including the Health Information Technology for Economic and Clinical Health Act ("HITECH") and the regulations issued by HHS on January 25, 2013. If Employer sponsors more than one health plan, the plans shall collectively be an organized health care arrangement under the HIPAA privacy and security rules in order to coordinate the operation of the plans and better serve the participants.

All employees of Employer who have access to PHI must comply with these Policies and Procedures. No third party rights (including but not limited to rights of Plan participants or business associates) are intended to be created by these Policies and Procedures. Employer reserves the right to amend these Policies and Procedures at any time (and even retroactively) without notice. These Policies and Procedures do not address privacy or security requirements under other federal or state laws.

These policies and procedures amend and restate Employer's prior policies and procedures and are effective as of September 23, 2013.

### II. Privacy Policies and Procedures

#### A. Procedures for Use and Disclosure of PHI

##### 1. Use and Disclosure Defined

The Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- a. *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for Employer, or by a business associate of the Plan.
- b. *Disclosure.* Any release, transfer, provision of access to, or divulging in any other manner of PHI to persons not employed by Employer.

##### 2. Access to PHI is Limited to Certain Employees

The following employees ("employees with access") have access to PHI:

City Manager  
Director Human Resources  
Finance Director  
Director of Information Technology  
Manager's Office, Finance, Human Resources and Information  
Technology Department Staff

## *HIPAA Policies And Procedures*

Directors, Department Heads and Supervisors (as appropriate)  
Mayor and City Council  
Retirement Board  
City Attorney

These employees with access may use and disclose PHI for Plan administrative functions, and they may disclose PHI to other employees with access for Plan administrative functions, subject to the requirement to disclose the minimum amount necessary to perform the Plan administrative functions (see Section II(A)(10)). For this purpose, Plan administrative functions means activities that would meet the definition of payment or health care operations, but do not include functions to modify, amend, or terminate the Plan or solicit bids from prospective issuers. Plan administrative functions include quality assurance, employee assistance, claims processing, auditing, monitoring, and management of carve-out-plans—such as vision and dental. PHI for these purposes may not be used by or between the Plan or business associates of the Plan in a manner inconsistent with the HIPAA privacy rules, absent an authorization from the individual. Plan administrative functions specifically do not include any employment-related functions. Employees with access may not disclose PHI to employees (other than employees with access) except in accordance with these Policies and Procedures.

### 3. Permitted Uses and Disclosures of PHI: Payment and Health Care Operations

#### a. *Definitions*

i. *Payment.* Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

(A) eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims; and

(B) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

## *HIPAA Policies And Procedures*

- ii. *Health Care Operations.* Health care operations means any of the following activities to the extent that they are related to Plan administration:
  - (A) conducting quality assessment and improvement activities;
  - (B) reviewing health plan performance;
  - (C) underwriting and premium rating;
  - (D) conducting or arranging for medical review, legal services and auditing functions;
  - (E) business planning and development; and
  - (F) business management and general administrative activities.

### b. *Procedure*

- i. *Uses and Disclosures for Plan's Own Payment Activities or Health Care Operations.* An employee may use and disclose a Plan participant's PHI to perform the Plan's own payment activities or health care operations subject to Section II(A)(10).
- ii. *Disclosures for Another Entity's Payment Activities.* An employee may disclose a Plan participant's PHI to another covered entity or health care provider to perform the other entity's payment activities subject to Section II(A)(10).
- iii. *Disclosures for Certain Health Care Operations of the Receiving Entity.* An employee may disclose PHI for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship subject to Section II(A)(10).
- iv. *Use or Disclosure for Purposes of Non-Health Benefits.* Unless an authorization from the individual (see Section II(A)(6)) has been received, a participant's PHI may not be used for the payment or operations of Employer's "non-health" benefits (e.g., disability and life insurance). If an

## *HIPAA Policies And Procedures*

employee requires a participant's PHI for the payment or health care operations of non-Plan benefits, follow these steps:

- (A) *Obtain an Authorization.* First, contact the Privacy Officer to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, ask the individual to complete and return an authorization form provided by (or approved by) the Privacy Officer.
- (B) The disclosure must comply with Sections II(A)(10) and (11).

### 4. Mandatory Disclosures of PHI to Individuals and HHS

- a. *Request From Individual.* Upon receiving a request from an individual (or from a minor's parent an individual's authorized personal representative) for disclosure of the individual's own PHI, follow Section II(B).
- b. *Request From HHS.* Upon receiving a request from the U.S. Department of Health and Human Services ("HHS") for disclosure of PHI, follow the procedures for verifying the identity of a public official set forth in Section II(A)(9).

### 5. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

- a. *Procedure.* If a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" the Privacy Officer must be contacted and the disclosure must comply with Section II(A)(10) and Section II(A)(11), if applicable.
- b. *Legal and Public Policy Disclosures Covered*
  - i. *Disclosures about victims of abuse, neglect or domestic violence,* if the following conditions are met:
    - (A) The individual agrees with the disclosure; or
    - (B) The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is

## *HIPAA Policies And Procedures*

necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

- ii. *For Judicial and Administrative Proceedings*, in response to:
  - (A) An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); or
  - (B) A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.
- iii. *To a Law Enforcement Official for Law Enforcement Purposes*, under one of the following conditions:
  - (A) Disclosure is pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.
  - (B) The information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.
  - (C) The information is about a suspected victim of a crime if the individual agrees to disclosure; or if the information is not to be used against the victim, the need for the information is urgent, and disclosure is in the best interest of the individual.
  - (D) The information is about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.

## *HIPAA Policies And Procedures*

- (E) The information constitutes evidence of criminal conduct that occurred on Employer's premises.
- iv. *To Public Health Authorities for Public Health Activities.*
- v. *To a Health Oversight Agency for Health Oversight Activities,* as authorized by law.
- vi. *To a Coroner or Medical Examiner About Decedents,* for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.
- vii. *For Cadaveric Organ, Eye or Tissue Donation Purposes,* to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.
- viii. *For Limited Research Purposes,* provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.
- ix. *To Avert a Serious Threat to Health or Safety,* upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.
- x. *For Specialized Government Functions,* including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities.
- xi. *For Workers' Compensation Programs,* to the extent necessary to comply with laws relating to workers' compensation or other similar programs or for purposes of obtaining payment for any health care provided to an injured or ill employee.

### 6. Disclosures of PHI Pursuant to an Authorization

Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required under these Policies and Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

*HIPAA Policies And Procedures*

- a. Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in Section II(A)(9).
- b. Verify that the authorization form is valid. Attached as Appendix 1 is a sample authorization form to provide to individuals. Valid authorization forms are those that:
  - i. Are properly signed and dated by the individual or the individual's representative;
  - ii. Are not expired or revoked (the expiration date of the authorization form must be a specific date or a specific time period (e.g., one year from the date of signature)), or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's coverage);
  - iii. Contain a description of the information to be used or disclosed;
  - iv. Contain the name of the entity or person authorized to use or disclose the PHI;
  - v. Contain the name of the recipient of the use or disclosure;
  - vi. Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
  - vii. Contain a statement regarding the possibility for a subsequent re-disclosure of the information.
- c. All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.
- d. Disclosures must be documented in accordance with Section II(A)(11).
- e. See sample authorization forms (Appendices 1, 2 and 3).
  - i. Appendix 1 – generic authorization to include in enrollment form. This language could be incorporated into the initial and annual open enrollment materials. If an employee and his/her spouse or other adult dependents provide this authorization, one time, it will be unnecessary to obtain additional authorization in the future. Some employers

## *HIPAA Policies And Procedures*

may opt for to use this approach with respect to the employee but may seek to use Appendix 2 with respect to spouses and adult dependents enrolled in the Plan (because they typically do not provide authorization in connection with the enrollment process).

- ii. Appendix 2 – stand-alone generic authorization form. This stand-alone form is drafted in a generic fashion for a variety of uses (both to permit general uses and disclosures and specific uses and disclosures). It is similar to Appendix 1 but is a stand-alone document.
- iii. Appendix 3 – stand-alone specific authorization form. This stand-alone form could be used by an individual plan participant to authorize uses and disclosures of PHI in connection with a specific aspect of plan administration (e.g., enrollment or one particular claim). While generally not required with respect to the individual’s own PHI, many plans are interested in securing this type of authorization from plan participants. However, if the Plan wants to disclose PHI to the participant’s spouse (e.g., in order to facilitate claims processing), the participant should be required to sign this authorization form.

### 7. Disclosure of PHI to Business Associates

- a. *Definition of Business Associate.* Pursuant to HIPAA, a Business Associate is a person or entity who:
  - i. creates, receives, maintains or transmits PHI in connection with providing services on behalf of the Plan; or
  - ii. provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.
- b. *Procedure.* All uses and disclosures by a “business associate” must be made in accordance with a valid business associate agreement. Before providing PHI to a business associate, employees must contact the Privacy Officer and verify that a business associate agreement is in place. The following additional procedures must be satisfied:
  - i. Disclosures must be consistent with the terms of the business associate agreement.

### *HIPAA Policies And Procedures*

- ii. Disclosures must comply with Section II(A)(10). (Under that procedure, each recurring disclosure will be subject to a separate policy to address the minimum necessary requirement, and each non-recurring disclosure must be approved by the Privacy Officer.)
8. Requests for Disclosure of PHI From Spouses, Family Members, and Friends

The Plan will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI. However, this does not preclude PHI from being disclosed in an explanation of benefits as part of the Plan's payment functions.

- a. If a request for disclosure of an individual's PHI is received from a parent of the individual and the individual is a minor child, or the authorized personal representative of the individual, then follow the procedure in Section II(A)(9). Once the identity of the parent or authorized personal representative is verified, proceed subject to Section II(B).
- b. If the request for disclosure of an individual's PHI is received from a spouse, parent (and the individual is an adult child), other family member or personal friend, once the identity of spouse, family member or personal friend is verified under Section II(A)(9), the disclosure is permitted, subject to Section II(B), in the following circumstances:
  - i. If the individual is present or available and has the capacity to make health care decisions, then the Plan may use or disclose the PHI if it is directly relevant to the involvement of the spouse, parent, family member or friend with the individual's care or payment related to the individual's care if the Plan obtains the individual's agreement, or the individual is provided with the opportunity to object and does not do so or the Plan can reasonably infer from the circumstances, based on professional judgment, that the individual does not object to the disclosure.
  - ii. If the person is not present for the use or disclosure or the person is incapacitated or it is an emergency, then the Plan may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual. For example, it may be permissible to disclose

## *HIPAA Policies And Procedures*

PHI to an incapacitated participant's family member who contacts the Plan to assist in resolving a claim or payment issue.

iii. In addition, it is permissible for the Plan to disclose PHI to a spouse, parent, family member or friend of a deceased individual in order to resolve claim or payment issues.

c. All other requests from spouses, parents, family members, and friends must be authorized by the individual whose PHI is involved (see Section II(A)(6)).

### 9. Verification of Identity of Those Requesting PHI

Steps should be taken to verify the identity and authority of individuals who request access to PHI if the identity or authority of such a person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of his or her minor child, an authorized personal representative, or a public official seeking access.

a. *Request Made by Individual.* When an individual requests access to his or her own PHI, the following steps should be followed:

i. Request a form of identification from the individual such as a valid driver's license, passport or other photo identification issued by a government agency.

ii. Verify that the identification matches the identity of the individual requesting access to the PHI. If there are any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, the Privacy Officer must be contacted.

iii. Make a copy of the identification provided by the individual and file it with the individual's designated record set.

iv. If the individual requests PHI over the telephone, the individual must verify his/her address and Social Security number.

b. *Request Made by Parent Seeking PHI of Minor Child.* When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:

### *HIPAA Policies And Procedures*

- i. Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.
  - ii. The disclosure may only be approved if it is not prohibited by state law. If the PHI relates to pregnancy, sexually transmitted disease, HIV/AIDS, sexual assault, mental health treatment or substance abuse treatment, applicable state law should be reviewed to confirm that disclosure is not prohibited.
  - iii. Disclosures must be documented in accordance with Section II(A)(11), if applicable.
- c. *Request Made by Authorized Personal Representative.* When a personal representative requests access to an individual's PHI, the following steps should be followed:
- i. Require a copy of a valid power of attorney or other valid documentation. If there are any questions about the validity of this document, seek review by the Privacy Officer.
  - ii. Make a copy of the documentation provided and file it with the individual's designated record set.
  - iii. Disclosures must be documented in accordance with Section II(A)(11), if applicable.
- d. *Request Made by Public Official.* If a public official requests access to PHI, and if the request is for one of the purposes set forth above in Sections II(A)(4) or (A)(5), the following steps should be followed to verify the official's identity and authority:
- i. If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
  - ii. If the request is in writing, verify that the request is on the appropriate government letterhead.
  - iii. If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation

### *HIPAA Policies And Procedures*

of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

- iv. Request a written statement of the legal authority under which the information is requested, or if a written statement would be impracticable, an oral statement of such legal authority.
- v. Obtain approval for the disclosure from the Privacy Officer.

#### 10. Minimum Necessary/Firewalls

- a. *General Operating Procedures.* Except as otherwise noted, when PHI is disclosed pursuant to these Policies and Procedures, the disclosure shall be limited to the minimum amount necessary. In applying the minimum necessary standard, the Plan must first consider whether a limited data set (partially de-identified data) can be used or disclosed before using or disclosing PHI. (A limited data set excludes certain basic identifying information such as an individual's name, Social Security number and address but may still include certain identifying information such as birthdate and dates of service.)

To satisfy the minimum necessary requirement and the requirement that the Plan establish adequate physical, administrative and electronic firewalls to safeguard the use and disclosure of PHI, the Plan shall maintain the following general operating procedures with respect to employees identified in Section II(A)(2):

- i. *Functions of Employees.* Employees identified in Section II(A)(2) may use or disclose PHI for Plan administrative functions. These employees should not also perform employment related-functions or functions relating to other employee benefits or employee benefit plans (such as disability and life insurance) ("employment functions"). However, if this is not administratively feasible, the employees for whom this is not administratively feasible shall be instructed to proceed with significant deliberation and to attempt to separate their decisions with respect to Plan administrative functions and employment functions with respect to each employee.

## *HIPAA Policies And Procedures*

### ii. *Verbal Communications*

- (A) *General Rules.* When employees identified in Section II(A)(2) are using or disclosing PHI, the name of the individual shall not be stated or if required to be stated, shall be stated as little as possible. Similarly, the medical condition of the individual shall not be stated or if required to be stated, shall be stated as little as possible.
- (B) *Face-to-Face Communications.* Any face-to-face communications by employees identified in Section II(A)(2) involving PHI shall not occur in open areas. Rather, communications shall occur in offices behind closed doors. If face-to-face communications in an office behind a closed door is not administratively feasible, communications shall occur using as much privacy as possible (for example, in a cubicle or behind a divider).
- (C) *Telephonic Communications.* Telephonic communication by employees identified in Section II(A)(2) shall not occur in open areas. Rather, communications shall occur in offices behind closed doors. If telephonic communications in an office behind a closed door is not administratively feasible, communications shall occur using as much privacy as possible (for example, in a cubicle or behind a divider). Employees identified in Section II(A)(2) shall not leave voice mail messages containing PHI.

### iii. *Written Communications*

- (A) Employees identified in Section II(A)(2) who are likely to receive PHI via mail shall be instructed to open their mail in a private place (such as at their desk) rather than in an open area. Once the mail is opened, it shall be kept in the individual's PHI file (see below). If there is no individual PHI file currently maintained for the individual, a new file shall be opened as soon as administratively feasible. If the mail needs to be forwarded, it shall be forwarded in a confidential envelope.

## *HIPAA Policies And Procedures*

- (B) PHI that is in the process of being used by employees identified in Section II(A)(2) should be used and stored in a confidential manner. Documents containing PHI should not be left out on an employee's desk during times such as breaks, lunch hours and at the end of the work day where the employee is not present and the documents may be viewed by others. If PHI is in the process of being used, the PHI should be stored out of sight during time periods when an employee is not at his or her desk.
- (C) A separate PHI file should be maintained for each individual. The PHI file should be kept apart from other personnel records concerning an employee. Individual PHI files should be stored in a separate file area. The file drawers and/or file room should be locked and access should be limited.
- (D) Identify all fax machines likely to receive PHI. The fax machine(s) should be in a secure location where access to employees is limited. The most minimal number of fax machines that is administratively feasible should be designated to receive PHI.
- (E) Paper copies of PHI may be maintained or destroyed, subject to the requirements in Section II(A)(11) below. If paper copies of PHI are maintained, they may continue to be held in the files described above or may be held in some other permanent storage area provided again that the area is secure and access is limited. Alternatively, PHI not required to be held may be destroyed. Destruction shall occur in a method such as shredding, burning, pulverizing or other destruction where the PHI cannot be read or otherwise reconstructed.

### *iv. Communications via Computer or E-mail*

- (A) Employees identified in Section II(A)(2) shall have their work stations and computer terminals located in areas to minimize the inadvertent disclosure of PHI. Work stations and computer terminals shall be located in offices. If offices are not administratively

## *HIPAA Policies And Procedures*

feasible, work stations and computer terminals shall be located in cubicles or behind dividers.

- (B) Access to the computer terminal of each employee identified in Section II(A)(2) shall be limited through the use of passwords and other appropriate privacy safeguards. Passwords shall be periodically changed.
  - (C) When PHI is stored or transmitted electronically, steps should be taken to minimize inadvertent disclosure such as using encryption, firewalls, passwords and other similar methods. If the Plan is a hybrid entity and offers non-health benefits, firewalls shall be established between the health benefit and non-health benefit portions of the Plan.
  - (D) If employees identified in Section II(A)(2) use or disclose PHI via computer or e-mail, their computer terminals shall be turned off or locked during time periods when they are away from their desk (such as during breaks, lunch hours and at the end of the work day). An automatic log-off or lockout system should also be utilized.
  - (E) Hard drives of the computer systems should be cleared or purged of data in the event a computer is discarded.
- b. *Routine and Recurring Disclosures of PHI.* For disclosures made on a routine and recurring basis, the PHI disclosed shall be limited to the amount reasonably necessary to achieve the purpose of the disclosure:
- i. *Third Party Administrator.* To perform its duties relating to the Plan, the Third Party Administrator shall have access to all information that is available to the Plan Administrator.
  - ii. *Decisions on Claims and Appeals.* Fiduciaries of the Plan who review claims decisions and/or claims appeals requiring the use of discretion shall have access to, and disclose, that amount of PHI as they may deem necessary, in the exercise of discretion and professional judgment, to render a claims determination or decide an appeal.

### *HIPAA Policies And Procedures*

- iii. *Eligibility Determinations.* For purposes of determinations of eligibility, the Plan fiduciaries shall have access to all enrollment information of Plan participants and those individuals who have applied for coverage under the Plan.
- iv. *Coverage Determinations.* For purposes of determinations of coverage, the Plan fiduciaries shall have access to the individual's claims file regarding the claim in question.
- v. *Coordination of Benefits.* For coordination of benefits purposes, the Plan fiduciaries and other health plans or health insurance providers shall have access to all enrollment information of the Plan participants who are the subject of the inquiry, as well as information regarding other coverage those participants may have.
- vi. *Human Resources/Benefits.* Human Resources and Benefits management and designated staff shall have access to information regarding claims filed, appeals filed, eligibility, enrollment, termination, COBRA coverage and applications for coverage, as necessary to supervise the day-to-day operations of the Plan and to assist participants with questions and concerns regarding their benefits under the Plan.
- vii. *Plan Auditor.* The Plan auditor shall have information regarding claims filed, PPO repricing, claims paid, stop-loss submittals, eligibility, enrollment, termination, COBRA participants, COBRA premiums, participant contributions and checking accounts, to audit the handling of funds related to the Plan as well as any Plan assets.
- viii. *Plan Operations.* The Plan fiduciaries shall have access to all information needed to oversee and make decisions concerning Plan operations, including claims costs, administrative costs, any stop-loss coverage and audit reports.
- ix. *Chief Financial Officer.* The Chief Financial Officer of the Plan Sponsor and the Plan Administrator shall have access to all information regarding funding and expenses of the Plan, including but not limited to information regarding claims filed, PPO re-pricing claim funding requirements, claims paid, stop-loss submittals, COBRA premiums, participant contributions and checking accounts.

### *HIPAA Policies And Procedures*

- x. *Plan Sponsor Audits.* For auditing purposes, the Plan Sponsor shall have access to claims information for the prior plan year, as well as information regarding specific claims as are requested to assess the Plan's performance and review Plan costs.
- xi. *Underwriting.* For underwriting purposes, the stop-loss carriers and managing general underwriters from whom quotes are obtained shall have access to aggregate claims information for the prior plan year, as well as such information regarding specific claims as are requested to determine the cause of unexpected claims that could influence the premium.
- xii. *Stop-Loss Claims.* Any stop-loss carrier and managing general underwriter shall have access to information regarding specific and aggregate claims as necessary to determine whether or not such claims are payable or reimbursable.
- xiii. *Utilization Review Companies.* Any utilization review companies used by the Plan shall have access to such medical records and medical information as they deem necessary to perform their duties related to pre-admission certification, concurrent review and retrospective review.
- xiv. *Attorneys.* For purposes of providing legal services to the Plan, the Plan's attorneys shall have access only to that class of an individual's PHI that relates to the issues on which the attorneys advise the Plan.
- xv. *Insurance Broker.* For purposes of providing advice to the Plan, its insurance broker shall have access to such eligibility, enrollment, termination, COBRA, claims and stop-loss information as necessary to provide accurate and complete advice.
- xvi. *Subrogation Vendor.* Any subrogation vendor used by the Plan shall have access to such medical records, accident information and claims information as it deems necessary to perform its duties relating to the Plan's subrogation interests.
- xvii. *COBRA Vendor.* Any vendor used by the Plan to provide COBRA administration services shall have access to such information relating to enrollment, eligibility, termination,

## *HIPAA Policies And Procedures*

COBRA elections and payment of COBRA premiums as it deems necessary to perform its duties for the Plan.

- xviii. *Preferred Provider Organization(s)*. Any preferred provider organizations providing discounted rates to the Plan shall have access to all claims relating to services provided by member providers so that it may re-price such claims and resolve any disputes in connection therewith.
- xix. *Printing and Mailing Services*. Any printing and mailing service used by the Plan shall have access to those documents to be printed and mailed, to perform its duties for the Plan.
- xx. *Scanning and Scrubbing Services*. Any scanning and/or claims “scrubbing” service(s) used by the Plan shall have access to the documents to be scanned and the Plan’s database in connection therewith, to perform the duties owed to the Plan.

For all other requests for disclosures of PHI, contact the Privacy Officer, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

### c. *Procedures for Requests*

- i. *Routine and Recurring Requests*. For requests made on a routine and recurring basis, implement and comply with the following policies and procedures that limit the PHI requested to the amount reasonably necessary to achieve the purpose of the request.
  - (A) *Plan Fiduciaries*. Fiduciaries of the Plan who review claims decisions and/or claims appeals requiring the use of discretion shall request only that amount of PHI as they may deem necessary, in the exercise of discretion and professional judgment, to render a claims determination or decide an appeal.
  - (B) *Eligibility Determinations*. For purposes of determinations of eligibility, the Plan Administrator shall request all enrollment information of Plan participants and those individuals who have applied for coverage under the Plan.

## *HIPAA Policies And Procedures*

- (C) *Coverage Determinations.* For purposes of determinations of coverage, the Plan Administrator shall request the individual's claims file regarding the claim in question.
- (D) *Coordination of Benefits.* For coordination of benefit purposes, the Plan Administrator and other health plans or health insurance providers shall request all enrollment information of the Plan participants who are the subject of the inquiry, as well as information regarding other coverage those participants may have.
- (E) *Human Resources / Benefits.* Human Resources / Benefits management and designated staff shall request information regarding claims filed, appeals filed, eligibility, enrollment, termination, COBRA coverage and applications for coverage, as necessary to supervise the day-to-day operations of the Plan and to assist participants with questions and concerns regarding their benefits under the Plan.
- (F) *Plan Auditor.* The Plan auditor shall request information regarding claims filed, PPO re-pricing, claims paid, stop-loss submittals, eligibility, enrollment, termination, COBRA participants, COBRA premiums, participant contributions and checking accounts, to audit the handling of funds related to the Plan as well as any Plan assets.
- (G) *Chief Financial Officer.* The Chief Financial Officer of the Plan Administrator shall request all information regarding funding and expenses of the Plan, including but not limited to information regarding claims filed, PPO re-pricing, claim funding requirements, claims paid, stop-loss submittals, COBRA premiums, participant contributions and checking accounts.
- (H) *Plan Operations.* The Plan Administrator shall request all information needed to oversee and make decisions concerning Plan operations, including claims costs, administrative costs, stop-loss premiums and provisions and audit reports.

*HIPAA Policies And Procedures*

- ii. For all other requests for PHI, contact the Privacy Officer, who will ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.
- d. *Exceptions.* The “minimum necessary” standard does not apply to any of the following:
  - i. Uses or disclosures made to the individual;
  - ii. Uses or disclosures made pursuant to an individual authorization;
  - iii. Disclosures made to HHS;
  - iv. Uses or disclosures required by law; and
  - v. Uses or disclosures required to comply with HIPAA.

11. Documentation

Copies of all of the following items shall be maintained for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- a. “Notices of Privacy Practices” that are issued to participants.
- b. Individual Authorizations
- c. An accounting log of all non-routine disclosures of PHI must be maintained.
  - i. For this purpose, the following disclosures of PHI are **not** considered non-routine:
    - (A) Disclosures to carry out treatment, payment or health care operations;
    - (B) Disclosures to an individual about his or her own PHI;
    - (C) Disclosures pursuant to an authorization;
    - (D) Disclosures for specific national security or intelligence purposes;

*HIPAA Policies And Procedures*

- (E) Disclosures to correctional institutions or law enforcement officials when the disclosure was permitted without authorization;
  - (F) Disclosures as part of a limited data set (relating primarily to research purposes); or
  - (G) Disclosures made before the Plan's HIPAA privacy compliance effective date.
- ii. For this purpose, the following disclosures of PHI **are** considered non-routine, requiring an accounting:
- (A) Accidental or erroneous disclosures (e.g., disclosures that shouldn't have been made);
  - (B) Disclosures required by law (e.g., reports to state or federal agencies or disclosures made to the Secretary of the HHS pursuant to the Secretary's authority to investigate the Plan's compliance with HIPAA);
  - (C) Disclosures about victims of abuse, neglect or domestic violence;
  - (D) Disclosures for judicial and administrative proceedings in response to a court order or subpoena;
  - (E) Disclosures for public health activities or health oversight activities;
  - (F) Disclosures to a coroner or medical examiner about decedents;
  - (G) Disclosures for cadaveric organ, eye or tissue donation purposes;
  - (H) Disclosures to avert a serious threat to health or safety;
  - (I) Disclosures for specialized government functions; and
  - (J) Disclosures to comply with workers' compensation laws.

### *HIPAA Policies And Procedures*

- iii. Notwithstanding the definition of non-routine disclosures in subsection (b) if the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, an accounting may not be required.
- iv. When a non-routine disclosure of PHI is made, the log should reflect:
  - (A) the date of the disclosure;
  - (B) the name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - (C) a brief description of the PHI disclosed;
  - (D) a brief statement of the purpose of the disclosure; and
  - (E) any other documentation required under these Policies and Procedures.

Attached as Appendix 4 is a sample disclosure log to be maintained for each individual for the accounting of non-routine disclosures of PHI.

#### 12. Disclosure of De-Identified Information

- a. *De-identified information* is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two approved, safe harbor ways the Plan can determine that information is de-identified: either by an expert determination which applies a professional statistical analysis, or by removing 18 specific identifiers. See 45 CFR 164.514(b).
- b. *Procedure*
  - i. Obtain approval from Privacy Officer for the disclosure to verify that the information is de-identified.

## *HIPAA Policies And Procedures*

- ii. The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

### B. Procedures for Complying With Individual Rights

#### 1. Request for Access to PHI Held in a Designated Record Set

- a. *Definition of Designated Record Set.* “Designated Record Set” means a group of records maintained by or for the Plan that includes:

- i. the enrollment, payment, claims adjudication and case or medical management record systems of an individual maintained by or for the Plan; or
- ii. other PHI used, in whole or in part, by or for the Plan to make decisions about an individual.

- b. *Procedure.* Upon receiving a written request from an individual (or from a minor’s parent or an individual’s authorized personal representative) for disclosure of an individual’s PHI held in a designated record set, the following steps must be followed:

- i. Follow the procedures for verifying the identity of the individual (or parent or authorized personal representative) set forth in Section II(A)(9).
- ii. Review the disclosure request to determine whether the PHI requested is held in the individual’s designated record set. See the Privacy Officer if it appears that the requested information is not held in the individual’s designated record set. No request for access may be denied without approval from the Privacy Officer.
- iii. Review the disclosure request to determine whether an exception to the disclosure requirement might exist. For example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, certain requests by inmates, information compiled during research when the individual has agreed to denial of access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. See the Privacy Officer if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Officer.

### *HIPAA Policies And Procedures*

- iv. Respond to the request by providing the information or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30- or 60-day period of the reasons for the extension and the date by which the Plan will respond.
  - (A) A denial notice must contain the basis for the denial, a statement of the individual's right to request a review of the denial, if applicable, and a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Officer.
  - (B) Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual. Individuals have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals also have the right to come in and inspect the information.
  - (C) If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.
- v. Disclosures must be documented in accordance with Section II(A)(11), if applicable.
- c. Effective September 23, 2013, an individual may request his or her PHI maintained as an electronic health record. An electronic health record means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff. It is unlikely that the Plan will hold any electronic health records regarding an individual. However, if such records are maintained by the Plan and the individual submits a request, the procedure set forth in subsection (b) shall apply in processing the request. In

### *HIPAA Policies And Procedures*

receiving these requests for PHI maintained as an electronic health record, the Plan shall consider the following:

- i. The Plan must provide the information in the form and format requested by the individual if the information is readily producible (e.g., in Word, Excel, etc.). If not readily producible, the Plan must provide the PHI in a readable electronic form such as PDF, as agreed to by the Plan and the individual.
- ii. The Plan is permitted to charge for labor and supplies, such as a flash drive.
- iii. An individual is permitted to designate a third party to receive the information. The designation must be in writing and signed by the individual.
- iv. The individual can request that the information be emailed, even if in a non-encrypted form.

## 2. Request for Amendment

Upon receiving a request from an individual (or a minor's parent or an individual's authorized personal representative) for amendment of an individual's PHI held in a designated record set, the Plan must take the following steps:

- a. Follow the procedures in Section II(A)(9).
- b. Review the disclosure request to determine whether the PHI at issue is held in the individual's designated record set. See the Privacy Officer if it appears that the requested information is not held in the individual's designated record set. No request for amendment may be denied without approval from the Privacy Officer.
- c. Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see Section II(A)(2)). See the Privacy Officer if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Officer.
- d. Review the request for amendment to determine whether the amendment is appropriate—that is, determine whether the

### *HIPAA Policies And Procedures*

information in the designated record set is accurate and complete without the amendment.

- e. Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Plan will respond.
- f. When an amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.
- g. When an amendment request is denied, the following procedures apply:
  - i. All notices of denial must be prepared or approved by the Privacy Officer. A denial notice must contain the basis for the denial, information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement, an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information, and a statement of how the individual may file a complaint concerning the denial.
  - ii. If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment, the denial notice of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

## *HIPAA Policies And Procedures*

### 3. Request for an Accounting of Uses and Disclosures of PHI

Upon receiving a request from an individual (or a minor's parent or an individual's authorized personal representative) for an accounting of non-routine uses and disclosures, the Plan must take the following steps:

- a. Follow the procedures set forth in Section II(A)(9).
- b. If the individual requesting the accounting has already received one accounting within the 12 month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request.
- c. Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Plan will respond.
- d. The accounting must include non-routine disclosures (but not uses) of the requesting individual's PHI made by the Plan and any of its business associates during the period requested by the individual up to six years prior to the request. (Note, however, that the plan is not required to account for any disclosures made prior to the Plan's HIPAA privacy compliance date.) The accounting will only include disclosures required by law and as a result, will not include disclosures made:
  - i. to carry out treatment, payment and health care operations;
  - ii. to the individual about his or her own PHI;
  - iii. pursuant to an individual authorization;
  - iv. for specific national security or intelligence purposes;
  - v. to correctional institutions or law enforcement when the disclosure was permitted without an authorization;

### *HIPAA Policies And Procedures*

- vi. as part of a limited data set (relating primarily to research purposes); and
  - vii. before the Plan's HIPAA privacy compliance effective date.
- e. If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Officer for more guidance.
- f. The accounting must include the following information for each reportable disclosure of the individual's PHI:
- i. the date of disclosure;
  - ii. the name (and if known, the address) of the entity or person to whom the information was disclosed;
  - iii. a brief description of the PHI disclosed; and
  - iv. a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)
- g. Accountings must be documented in accordance with Section II(A)(11).
- h. Effective as of such date as prescribed by HHS regulations, an individual may request an accounting of uses and disclosures of his or her PHI maintained as an electronic health record even if for treatment, payment or health care operations purposes during the three-year period that preceded the request. An electronic health record means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff. It is unlikely that the Plan will maintain any electronic health records regarding an individual. However, if such records are maintained by the Plan and the individual submits a request, the procedure set forth in the above subsections shall apply in processing the request.

#### 4. Request for Confidential Communications

### *HIPAA Policies And Procedures*

Upon receiving a written request from an individual (or a minor's parent or an individual's authorized personal representative) to receive communications of PHI by alternative means or at alternative locations, the Plan must take the following steps:

- a. Follow the procedures set forth in Section II(A)(9).
- b. Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
- c. The Plan should take steps to honor requests which demonstrate that disclosure could endanger the individual.
- d. If a request will not be accommodated, the Plan must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- e. All confidential communication requests that are approved must be kept in a file maintained by the Privacy Officer.
- f. Requests and their dispositions must be documented in accordance with Section II(A)(11).

#### 5. Request for Restrictions on Uses and Disclosures of PHI

Upon receiving a written request from an individual (or a minor's parent or an individual's authorized personal representative) for restrictions on the use of disclosure of an individual's PHI, the Plan must take the following steps:

- a. Follow the procedures set forth in Section II(A)(9).
- b. The Plan should take steps to honor reasonable requests which demonstrate the need for the restrictions.
- c. If a request will not be accommodated, the Plan must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- d. All requests for limitations on use or disclosure of PHI that are approved must be kept in a file maintained by the Privacy Officer.
- e. Requests and their dispositions must be documented in accordance with Section II(A)(11).

## *HIPAA Policies And Procedures*

- f. Please note that an individual may request that a covered entity which is a health care provider restrict the disclosure of PHI to a health plan for payment or health care operations purposes where the individual has paid out-of-pocket in full for the service. This right to restrict disclosure generally does not apply directly to a health plan.

### C. Ongoing Compliance

#### 1. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under the HIPAA privacy rules. No individual shall be required to waive his or her rights under the HIPAA privacy rules as a condition of treatment, or Plan payment, enrollment or eligibility.

#### 2. Complaints

The Privacy Officer shall be the Plan's contact for receiving complaints. The Privacy Officer shall create a process for individuals to lodge complaints about these Policies and Procedures and a system for handling the complaints.

#### 3. Sanctions for Non-Compliance

Sanctions for non-compliance for employees identified in Section II(A)(2) shall be consistent with Employer's other disciplinary policies in connection with employee breaches of confidentiality. Disciplinary action shall be applied as appropriate and may include actions up to and including termination of employment. Business associates shall be sanctioned in accordance with the business associate agreement.

#### 4. Mitigation of Inadvertent Disclosures of PHI

HIPAA requires that the Plan mitigate, to the extent possible, any harmful effects that become known of a use or disclosure of an individual's PHI in violation of these Policies and Procedures. As a result, if an employee becomes aware of a disclosure of PHI, either by another employee or a business associate or other outside party, that is not in compliance with these Policies and Procedures, the employee is directed to contact the Privacy Officer as soon as possible so that the appropriate steps to mitigate the harm to the individual can be taken.

## *HIPAA Policies And Procedures*

### III. Security Policies and Procedures for Electronic PHI

The Plan shall adopt the following policies and procedures to comply with the security standards and implementation specifications of the HIPAA security rules regarding electronic PHI.

#### A. Electronic PHI Defined

Electronic PHI or ePHI is a smaller subset of PHI that is transmitted by or maintained in electronic media, such as computers, magnetic tape or disk, optical disk, digital memory card, internet, extranet, leased lines, dial-up lines and private networks. This can potentially include voicemail digitally produced from an information system and transmitted by phone.

These security policies and procedures not only apply to electronic media housed at Plan Sponsor's physical sites, it also applies to any mobile devices, such as iPhones, Android phones, iPads, tablets, etc. and any other electronic media used by Plan Sponsor's workforce offsite.

#### B. Security Management Process

1. The Plan shall identify the types of ePHI it transmits/maintains and the hardware, software, system interfaces, data and personnel involved. If the ePHI is not necessary for treatment, payment or health care operations purposes relating to the Plan then the Security Officer or designee shall direct that the ePHI no longer be transmitted or maintained.
2. The Plan shall conduct an analysis to assess potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI. The analysis shall be documented. The risks and vulnerability include the following:
  - a. Natural disasters;
  - b. Fires;
  - c. Electrical outages;
  - d. System malfunctions;
  - e. Viruses;
  - f. Hackers; and
  - g. Personnel error and/or lack of training.

## *HIPAA Policies And Procedures*

For each risk and vulnerability the Plan shall evaluate current security protection in place (e.g., in the case of viruses-anti-virus software, or in the case of personnel error and/or lack of training-training.)

3. If the security protections identified above are not adequate to reduce the risk or vulnerability of a likely threat to a reasonable and appropriate level, the Plan shall identify and implement appropriate additional security measures.
4. If employees do not comply with these security policies and procedures, the sanction for non-compliance identified in the HIPAA privacy policies and procedures shall apply.
5. The Plan shall utilize a proactive notification of security incidents and system events, which is triggered by automated monitoring tools.

### C. Workforce Security

1. The Plan shall identify the employees or classes of employees with authority to work with ePHI which shall include the following:

City Manager  
Director of Human Resources  
Finance Director  
Director of Information Technology  
Manager's Office, Finance, Human Resources and Information  
Technology Department Staff  
Directors, Department Heads and Supervisors (as appropriate)  
Mayor and City Council  
Retirement Board  
City Attorney

2. Appropriate background checks shall be conducted with respect to new hires that will be given authority to work with ePHI.
3. When the employment of an employee who has authority to work with PHI is terminated or the employee is no longer authorized to work with ePHI, the employee's means of access to ePHI shall be recovered (e.g., identification badge, access cards, etc.) and the individual's user identification and password shall be deactivated.

### D. Information Access Management

1. For the employees or classes of employees listed in Section III(C)(1), the Plan shall determine an employee's authority to work with ePHI through

## *HIPAA Policies And Procedures*

access to a work station, transaction, program and/or process. Authority for access may be identity-based, role-based and/or location-based.

2. Any existing access controls shall be reviewed and modified as necessary to ensure that each employee's right of access to ePHI satisfies the minimum necessary standards of the privacy rule.

### E. Security Awareness and Training

1. The employee or classes of employees identified in Section III(C)(1) who shall be authorized to work with ePHI shall receive training to comply with the HIPAA security rule. The training can be part of or in addition to the training provided regarding the HIPAA privacy rule. The training shall include periodic reminders regarding the security rule. Employees shall be provided with a copy of these policies and procedures as part of the training.
2. Training shall include instruction regarding the following:
  - a. How to guard against, detect and report malicious software, such as viruses. For example, employees should be instructed not to open suspicious e-mail. Any reporting should be made to the Security Officer or designee.
  - b. How to detect and report unsuccessful logins and discrepancies. Any reporting should be made to the Security Officer or designee.
  - c. How to create, change and safeguard passwords (e.g., passwords should not be posted next to the individual's computer screen, but rather, should be kept in a secure, separate location).

### F. Security Incident Procedures

1. The security rules require the Plan to implement policies and procedures to address security incidents. A "security incident" is an attempted or successful unauthorized access, use, disclosure, modification or destruction of ePHI, or the interference with system operations in an information system holding ePHI.
2. Suspected or known security incidents shall be promptly reported to the Security Officer or designee. The Security Officer or designee shall investigate and mitigate, to the extent practicable, any harmful effects of any known security incidents. The Security Officer or designee shall also document security incidents and their outcomes.

### G. Contingency Plan

### *HIPAA Policies And Procedures*

1. The data back-up plan, disaster recovery plan and emergency mode operations plan described in this Section shall constitute the Plan's contingency plan for purposes of the HIPAA security rules.
2. Plan Sponsor maintains a data back-up plan to create and maintain retrievable copies of data in the event of an emergency or other occurrence (e.g., a fire, vandalism, system failure or natural disaster). The data back-up plan shall be modified to specifically include ePHI held by the Plan and/or Plan Sponsor which will allow the Plan to continue business as usual. However, if the ePHI is also held by a business associate or subcontractor, that shall constitute a sufficient data back-up plan.
3. Plan Sponsor maintains a disaster recovery plan to restore lost data in the event of an emergency or other occurrence. The disaster recovery plan shall be modified to specifically include ePHI held by the Plan and/or Plan Sponsor which will allow the Plan to continue business as usual. However, if the ePHI is also held by a business associate or subcontractor, that shall constitute a sufficient disaster recovery plan.
4. Plan Sponsor maintains an emergency mode operations plan. The emergency mode operations plan shall be modified to specifically address the continuation of business processes for protection of the security of ePHI while the Plan and/or Plan Sponsor operate in an emergency mode.
5. Certain applications and data are the most critical in support of a contingency plan. Plan Sponsor has made this determination with respect to the data back-up plan, disaster recovery plan and emergency mode operations plan. Plan Sponsor shall modify this determination to specify which applications and data (such as firewalls and anti-virus software) are the most critical to protect the security of ePHI in a contingency plan.

#### H. Evaluation

1. The Security Officer or designee shall direct periodic technical and non-technical evaluations of the components of the security policies and procedures to be performed. Examples of technical evaluations may include reviewing and/or auditing systems logs or results of penetration testing. Examples of non-technical evaluations may include interviews or surveys.
2. If the Plan's security operations or security environment significantly changes, a new evaluation should occur.
3. The Security Officer or designee shall document the results of each evaluation.

## *HIPAA Policies And Procedures*

### I. Facility Access Controls

1. As part of the disaster recovery plan and emergency mode operations plan, Plan Sponsor shall establish procedures that allow facility access. The disaster recovery plan and emergency mode operations plan shall be revised to provide for access to permit appropriate employees or business associates or subcontractors to perform necessary functions involving ePHI following an emergency or other occurrence.
2. The facilities housing PHI shall be safeguarded to prevent unauthorized physical access, tampering and theft. Facilities should be secured through various devices which may include traditional key operated locks, electronic locks with magnetic cards or biometric recognition devices, window locks, lighting, motion detectors, fences, guards and alarms.
3. The Security Officer or designee shall ensure that only authorized persons have access to facilities housing PHI based on their role or function. For example, employees with access to the server room may be issued a key to that room. Non-employees with access (such as a business associate) may gain access by registering with a receptionist or other designated employee.
4. The Security Officer or designee shall maintain records to document repairs and modifications to a facility housing ePHI which relate to security, such as changes to locks, doors and walls.

### J. Work Station Use and Work Station Security

1. Proper uses of work stations (e.g., desk top computers and lap top computers) shall be specified in Plan Sponsor's information systems policy. For each work station or class of work station, the Security Officer or designee shall review the physical attributes of the surroundings. If the work station is located in an open area or cubicle, the location of the screen or the location of the entire work station may need to be moved or a privacy computer filter may need to be attached to the monitor to protect the security of ePHI. For employees using lap tops in varied locations, the employees shall be trained to use the laptop in a private area when accessing ePHI.
2. Training shall include reminders to employees with work stations housing ePHI to log off during periods when away from their work stations and to close out their screens when interrupted while working with ePHI.
3. If the physical location of any work station or class of work station which houses ePHI makes the work station unreasonably vulnerable to access by unauthorized users, the Security Officer or designee shall review and

## *HIPAA Policies And Procedures*

consider implementation of changes to address the necessary physical safeguards. Safeguards may include housing workstations in locked or secured areas and/or installing means of identifying Plan Sponsor's ownership of the workstation to facilitate recovery in the event of theft.

### K. Device and Media Controls

1. Plan Sponsor maintains a policy regarding the removal of confidential information from computer hardware and electronic media before it is disposed of or reused. The policy shall be modified to specifically address the removal of ePHI from the computer hardware or electronic media in these situations. For example, to remove ePHI before a laptop computer is reused, the "secure delete" capability with byte-for-byte overwrite would be an appropriate means of deleting the ePHI.
2. The Security Officer or designee shall maintain a record of the movement of computer hardware and electronic media containing ePHI.
3. If there is a risk of losing ePHI before equipment is moved, the Security Officer or designee shall ensure that a retrievable copy of the ePHI is created before the piece of equipment is moved. Before a piece of equipment is moved, the person responsible for the movement shall contact the Security Officer or designee in order for the determination to be made and any necessary action to be taken.

### L. Access Control

1. Each employee with authority to work with ePHI shall be assigned a unique user name and/or number.
2. The unique user name and/or identifying number system shall be designed in such a manner to enable the necessary personnel to continue to gain access to needed ePHI in an emergency.
3. If Plan Sponsor has not done so already, the Security Officer or designee shall ensure that electronic procedures such as automatic log off or inactivity lockout features be implemented to terminate an electronic session including ePHI after a predetermined time of inactivity.
4. Encryption is 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. The Security Officer or designee shall review the nature and volume of the ePHI being transmitted and the financial and technical burdens associated with encryption and after considering the same may determine it is necessary to implement a

## *HIPAA Policies And Procedures*

mechanism to encrypt/decrypt ePHI in order to protect the security of ePHI.

### M. Audit Controls, Integrity and Person or Entity Authentication

1. The Plan shall have in place hardware, software and/or procedural mechanisms to record and examine activity in information systems that store or use ePHI.
2. The Plan shall implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. Examples of permissible mechanisms to comply with this standard include password systems and telephone call back.

## IV. Breach Notification Procedures

If the security of unsecured PHI is breached, the Plan shall provide notice within the time period prescribed by law after the breach is discovered to the affected individual(s), HHS and the media as described below.

### A. Definitions

The following definitions apply for purposes of the Plan's breach notification procedures:

1. *"Unsecured"* PHI is all PHI except ePHI secured through encryption, and ePHI or paper PHI that has been destroyed. HHS has issued guidance prescribing acceptable encryption and destruction technologies and methodologies for this purpose.
2. *"Breach"* means the unauthorized acquisition, access, use or disclosure of unsecured PHI that compromises the privacy or security of the information. In order for a breach to occur, the acquisition, access, use or disclosure must be in violation of the HIPAA privacy rules.
3. *"Discovery"* occurs as of the first day on which the breach is known or by exercising reasonable diligence would have been known to the Plan, or if earlier, the day on which any workforce member (e.g., employee, volunteer, trainee, etc.) or other agent has knowledge of the breach or by exercising reasonable diligence would have knowledge (except for the individual who committed the breach).
4. *"Time period prescribed by law"* means without unreasonable delay and in no case later than 60 calendar days. Sixty calendar days of the breach should be considered an outer limit and depending on the circumstances, it

## *HIPAA Policies And Procedures*

may be an unreasonable delay to wait until the 60<sup>th</sup> day to provide notification.

### B. Other Issues to Consider Before Breach Notification is Required

1. *No notification if low probability of compromise.* A breach of unsecured PHI is presumed unless the Plan demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- b. The unauthorized person who used the PHI or to whom the disclosure was made;
- c. Whether the PHI was actually acquired or viewed; and
- d. The extent to which the risk PHI has been mitigated.

The Plan should conduct an assessment to determine if the low probability standard is met and should document the determination.

2. *Exceptions.* If the Plan discovers a breach of unsecured PHI but it falls within one of the following three exceptions, no notification is required:

- a. First, any unintentional acquisition, access or use of PHI by a workforce member (employee, volunteer, trainee, etc.) or person acting under the authority of a covered entity or business associate, if the acquisition, access or use was made in good faith and within the scope of the person's duties and does not result in further use or disclosure in violation of the privacy rules. For example, a co-worker mistakenly sends an email with PHI to another co-worker who opens it in the normal course of business but then deletes it and notifies the first employee.
- b. Second, an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another similarly situated person authorized to access PHI at the same covered entity or business associate and the information is not further used or disclosed in violation of the HIPAA privacy rules. For example, an employee of business associate for health plan A is working on-site at Plan Sponsor and Plan Sponsor's benefit manager inadvertently discloses PHI to the employee regarding health plan B.

## *HIPAA Policies And Procedures*

- c. Third, a disclosure of PHI where a covered entity or business associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. For example, two Jane Smiths work for the same employer. A Human Resources employee provides an enrollment form or explanation of benefits regarding the health plan to the wrong Jane Smith, recognizes the error and immediately takes back the document.

### C. Notification Steps

If unsecured PHI has been breached and a determination has been made that there is a significant risk of harm and no exception applies, the affected individual(s), HHS and the media should be notified as described below.

#### 1. Individual Notice

The affected individual(s) should be notified within the time period prescribed by law after discovery of the breach.

- a. *Content.* The content of the individual notice must be written in plain language and must include the following:
  - i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  - ii. 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);
  - iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
  - iv. A brief description of what the Plan is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and
  - v. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, email address, website or postal address.
  - vi. See Appendix 4 and 5 for samples.

## *HIPAA Policies And Procedures*

### b. *Method of Notice*

- i. Generally, the individual notice should be provided in writing by first-class mail to the individual's last known address. If multiple affected individuals reside at the same address, one notice can be sent.
- ii. Alternatively, written notice may be in the form of email provided the individual agrees to receive electronic notice and such agreement has not been withdrawn.
- iii. If the individual is a minor or legally incapacitated, notice to the parent or personal representative is acceptable.
- iv. If the individual is deceased, notice must be sent to the last known address of the next of kin.
- v. If the Plan does not have sufficient contact information for some or all of the affected individuals or if some of the notices are returned as undeliverable, substitute notice should be provided to the unreachable individuals in a manner reasonably calculated to reach them. For example, if the Plan does not have the individual's last known address, but has the individual's email or telephone number, notice can be provided electronically or by phone without the individual's consent. Posting a notice on Employer's website may also be appropriate.

If the Plan has insufficient contact information for ten or more affected individuals, the Plan must either post a conspicuous notice on the home page of Employer's website for at least 90 days or a conspicuous notice must be made in major print or broadcast media in the geographic area(s) where the affected individuals likely reside. The notice must include a toll-free telephone number that remains active for at least 90 days for individuals to call regarding the breach.

- vi. If the Plan determines that because of imminent possible misuse of the unsecured PHI, immediate notice is necessary, immediate contact such as by telephone can be made in addition to the normal individual notice which is required.

## 2. HHS Notice

## *HIPAA Policies And Procedures*

- a. *Breaches involving less than 500 individuals.* The Plan must maintain a log or other documentation of the breaches and submit the information annually to HHS for breaches occurring during the preceding calendar year. The information will be required to be submitted within 60 calendar days after the end of each calendar year. The information required will be specified by HHS on its website (HHS.gov). The internal log must be kept for six years. A sample log to use for this purpose is attached as Appendix 6.
- b. *Breaches involving 500 or more individuals.* The Plan must notify HHS immediately by following instructions on the HHS website (HHS.gov) and HHS will identify the Plan on its website. For this purpose, “immediately” means contemporaneously with the individual notice(s).

### 3. Media Notice

Notice to the media is only required where a breach of unsecured PHI is reasonably believed to affect more than 500 individuals in a state. In this circumstance, the Plan must provide notice to prominent media outlets, such as a general interest newspaper with daily circulation covering the area where the affected individuals live.

- a. The same content as the individual notice must be provided and within the same timeframe.
- b. The notice can be in a form of a press release.

### D. Business Associates

1. If a business associate discovers the breach, it must notify the Plan without unreasonable delay and within any time period prescribed by the business associate agreement which shall generally be in no event be later than 60 days after discovery (but see last sentence of this paragraph). For this purpose, “discovery” means the first day on which the breach is known to the business associate or by exercising reasonable diligence would have been known to the business associate. A business associate will be deemed to have knowledge of a breach if the breach is known or by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is an employee, officer, subcontractor or other agent of the business associate. However, if the business associate is acting as an agent for the covered entity, the business associate must notify the covered entity as soon as possible because the business associate and covered entity are treated as one for purposes of the 60-day time limit described in Section IV(A)(4).

### *HIPAA Policies And Procedures*

The notification must include identification of each individual whose unsecured PHI has been or has reasonably believed to have been breached and any other available information in its possession which the Plan is required to include in the individual notice.

- a. The Plan and the business associate may agree, pursuant to the business associate agreement, that the business associate will assume the notice obligation on behalf of the Plan in the following circumstances.
  - i. Where a breach of unsecured PHI was committed by the business associate or an employee, officer, subcontractor or other agent of the business associate or is within the unique knowledge of the business associate, as opposed to the Plan, the parties may agree pursuant to the business associate agreement that the business associate will provide the notice to the affected individuals. However, in this situation, the parties may further agree that the Plan shall have the right to promptly review and approve of any notices before sent and that such approval shall not be unreasonably withheld.
  - ii. Where a breach involves more than 500 individuals and where the breach was committed by the business associate or an employee, officer, subcontractor or other agent of the business associate or is within the unique knowledge of the business associate, as opposed to the Plan, the parties may agree pursuant to the business associate agreement that the business associate shall provide notice to the media. Again, the parties may further agree that Plan shall have the right to promptly review and approve of any notice before sent and that such approval shall not be unreasonably withheld.
- b. Where required by the business associate agreement, the business associate shall maintain its own log of breaches of unsecured PHI with respect to the Plan and shall submit the log to the Plan within 30 days following the end of each calendar year so that the Plan may report the breaches to HHS.

#### E. Law Enforcement

If an law enforcement individual indicates to the Plan or a business associate that a breach notification would impede a criminal investigation or cause damage to national security, the covered entity or business associate shall delay in providing the notice by up to 30 days from the date of the law enforcement official's

*HIPAA Policies And Procedures*

statement unless a longer time period is specified in any written document supplied by the law enforcement official.

**APPENDIX 1**

**Authorization for Release of Protected Health Information  
Health Plan(s) of the City of Wyoming**

By signing below, as an employee or adult dependent, I authorize the use or disclosure of my individually identifiable health information by or to any family member, member of my household, any health care provider, the plan sponsor, the insurer/TPA of the plan, or any other entity providing services in connection with the plan sponsor in order to process my enrollment in the plan or to process any claim for my plan benefits. I also authorize the use or disclosure of my individually identifiable health information to send me marketing communications regarding products or services in connection with the plan. This authorization is effective until the date I terminate enrollment in the plan. I have read and I understand the following: (1) I may revoke this authorization at any time before its expiration date by notifying the plan in writing, but the revocation will not have any effect on any actions the plan took before it received the revocation; (2) I may see and copy the information described on this authorization if I ask for it; (3) I am not required to sign this authorization to receive my health care benefits (enrollment, treatment, or payment); and (4) The information that is used or disclosed pursuant to this authorization may be re-disclosed by the receiving entity.

Employee Printed Name and Signature	Date Signed
Dependent Printed Name and Signature	Date Signed
Dependent Printed Name and Signature	Date Signed
Dependent Printed Name and Signature	Date Signed

**APPENDIX 2**

**Authorization for Release of Protected Health Information  
Health Plan(s) of the City of Wyoming**

I. Information About the Use or Disclosure

Individual's name: \_\_\_\_\_

This authorization relates to the health plan(s) of \_\_\_\_\_ (hereinafter referred to as the "Plan"). I authorize the use or disclosure of my individually identifiable health information by or to any family member or member of my household, health care provider, the Plan sponsor, the insurer/TPA of the Plan, or any other entity providing services in connection with the Plan in order to process my enrollment in the Plan or to process any claim for my Plan benefits. I also authorize the use or disclosure of my individually identifiable health information to send me marketing communications regarding products or services in connection with the Plan. This authorization is effective until the date I terminate enrollment in the Plan.

II. Important Information About Your Rights

I have read and understood the following statements about my rights:

- I may revoke this authorization at any time prior to its expiration date by notifying the Plan in writing, but the revocation will not have any affect on any actions the Plan took before it receive the revocation.
- I may see and copy the information described on this form if I ask for it.
- I am not required to sign this form to receive my health care benefits (enrollment, treatment, or payment).
- The information that is used or disclosed pursuant to this authorization may be redisclosed by the receiving entity.

III. Signature of Individual or Individual's Representative

\_\_\_\_\_  
Signature of Individual or Individual's Date  
Representative (Form MUST be completed before signing.)

Printed name of the Individual's personal representative: \_\_\_\_\_

Relationship to the individual, including authority for status as representative: \_\_\_\_\_

**APPENDIX 3**

**Authorization for Release of Protected Health Information  
Health Plan(s) of the City of Wyoming**

I. Information About the Use or Disclosure

I hereby authorize the use or disclosure of my individually identifiable health information from the Plan as described below. I understand that this authorization is voluntary and that I may revoke it at any time by submitting my revocation in writing to the Plan.

Individual's name: \_\_\_\_\_

Persons/organizations authorized to receive the information: \_\_\_\_\_

\_\_\_\_\_

Specific description of information to be used or disclosed: \_\_\_\_\_

\_\_\_\_\_

Specific purpose of the disclosure: \_\_\_\_\_

\_\_\_\_\_

This authorization will expire \_\_\_\_\_ (indicate date, or an event relating to you personally or to the purpose of the authorization).

II. Important Information About Your Rights

I have read and understood the following statements about my rights:

- I may revoke this authorization at any time prior to its expiration date by notifying the Plan in writing, but the revocation will not have any affect on any actions the Plan took before it receive the revocation.
- I may see and copy the information described on this form if I ask for it.
- I am not required to sign this form to receive my health care benefits (enrollment, treatment, or payment).
- The information that is used or disclosed pursuant to this authorization may be redisclosed by the receiving entity.

*HIPAA Policies And Procedures*

III. Signature of Individual or Individual's Representative

---

Signature of Individual or Individual's Representative (Form MUST be completed before signing.) \_\_\_\_\_ Date \_\_\_\_\_

Printed name of the Individual's personal representative: \_\_\_\_\_

Relationship to the individual, including authority for status as representative: \_\_\_\_\_



**APPENDIX 5**  
**Sample Individual Notice for Breach Notification**  
**[Employer Letterhead]**

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Re: Notice of Breach of Unsecured Protected Health Information

Dear \_\_\_\_\_:

The purpose of this letter is to notify you that certain personal information relating to your participation in the following health plan(s) maintained by \_\_\_\_\_ (“Employer”) has been breached or compromised: \_\_\_\_\_ [list Plan(s)] (“Plan”).

**What Happened?** [You should briefly explain what happened, including the date of the breach and the date of the discovery of the breach, if known.]

Example: On November 1, 2013, your annual open enrollment packet for the 2014 plan year was inadvertently sent to another Plan participant. The breach was discovered on November 7, 2013 when the other Plan participant contacted Employer’s HR department.

**Type of Personal Information Involved in the Breach** [You should explain 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.]

Example: The annual open enrollment packet contained your full name, Social Security number, date of birth, home address and Plan ID number. The packet also contained this same information regarding your dependents. [Remember, each such dependent would also be entitled to a notice but the notice for any minor children can be sent to the employee.] However, the packet did not contain any information regarding a medical diagnosis or treatment.

**Steps You Should Take** [The below example is where there is the risk of personal identity theft. Where only medical information is enrolled, this section could be completed simply to indicate the individual should be aware of this disclosure in the event the information is disseminated to others.]

Example: The disclosure of this personal information could potentially lead to a third party’s theft of your identity for illegal purposes. You should closely monitor your credit cards, bank accounts, etc. to make sure no one is attempting to gain access to your financial credit cards and accounts. Also, you should contact a credit monitoring service to make sure third parties are not improperly using your information to set up new credit cards, bank accounts, etc. for their use.

APPENDIX 5

**Sample Individual Notice for Breach Notification**  
**[Employer Letterhead]**

**Steps Plan is Taking** [You should briefly describe what the Plan is doing to investigate the breach, to mitigate harm to the individual and to protect against future breaches.]

Example: As soon as the Plan discovered the breach, it took the following steps:

V. The Plan asked the other Plan participant to immediately return the packet and instructed the Plan participant not to use or share the information.

VI. The Plan secured an identity theft insurance policy on your behalf for the next three months.

VII. The Plan conducted an internal investigation to determine what caused the breach and determined it was due to a manual sorting error in the mailing process. Since the breach has been discovered, the Plan has modified its procedures to minimize the risk of this issue occurring in the future.

**Contact Information** We apologize for this situation and any hardship or inconvenience it has placed upon you. If you have any questions regarding the incident or regarding any of the information described in this notice, please contact the Plan:

[Employer Name]  
[Address]  
[Address]  
Contact Person: \_\_\_\_\_  
Telephone No.: \_\_\_\_\_  
Email Address: \_\_\_\_\_

Sincerely,

[Employer]

By \_\_\_\_\_

Its \_\_\_\_\_

*HIPAA Policies And Procedures*

**APPENDIX 6**

**Log for Covered Entity to Document Breaches Required to be Disclosed Annually to the U.S. Department of Health & Human Services (“HHS”)**

**Health Plan(s) of the City of Wyoming**

The information to be disclosed and the procedure for disclosure will be set forth on the HHS website (HHS.gov).

<b><u>Date of Breach</u></b>	<b><u>Affected Individual(s)</u></b>	<b><u>Date of Discovery</u></b>

Attached to each entry should be a copy of the individual notice(s) sent in connection with the breach.