HIPAA PRIVACY POLICY

Introduction

City of La Crosse (the "Employer") sponsors the following group health plans:

- City of La Crosse Self-Funded Medical Benefit Plan
- City of La Crosse Section 125 Cafeteria Plan

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) these plans are considered to be "covered entities." For purposes of this Privacy Policy, the plans listed above are referred to collectively and singularly as the "Plan." Members of the Employer's workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan; or (2) on behalf of the Employer, for administrative functions of the Plan.

HIPAA as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and its implementing regulations restrict the Employer' ability to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

It is the Employer's policy to comply fully with HIPAA's requirements for the privacy of PHI. To that end, all members of the Employer's workforce who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Employer's more detailed use and disclosure procedures, the Employer's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Employer, whether or not they are paid by the Employer. The term "employee" includes all of these types of workers.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The Employer reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Employer. This Policy does not address requirements under other federal laws or under state laws.

Hybrid Entity. In accordance with the HIPAA privacy regulations, the City of La Crosse has designated the City as a Hybrid Entity. Given this designation, employment records and other City records other than those related to the covered Health Plan will not be considered to be PHI, subject to HIPAA requirements, unless specifically required by law. The Hybrid Election Form states the

following records are not subject to the HIPAA privacy regulations: information obtained to determine an individual's suitability to perform his/her job duties (such as physical examination reports) fit for duty exams, drug and alcohol tests obtained in the course of employment, doctor's excuses provided in accordance with the City of La Crosse's attendance policy, work-related injury and occupational exposures reports and medical and laboratory reports related to such injuries or exposures, including information necessary to determine worker's compensation coverage. Notwithstanding the fact that the preceding records are not subject to the HIPAA privacy regulations, it is the policy of the City of La Crosse to limit the use and disclosure of non-covered medical records only to those individuals who have a need to access them.

Plan's Responsibilities as Covered Entity

I. Privacy Official and Contact Person

The Employer shall designate the individual responsible for the human resource function of the Employer as the Privacy Officer.

The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Employer's more detailed use and disclosure procedures. The Privacy Official will also appoint those employees who will serve as the contact persons for participants who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Official is responsible for ensuring that the Plan complies with the provisions of the HIPAA privacy rules regarding business associates, including the requirement that the Plan have a HIPAA-compliant Business Associate Agreement in place with all business associates. The Privacy Official shall also be responsible for monitoring compliance by all business associates with the HIPAA privacy rules and this Privacy Policy.

Privacy Official is:
Deputy Director of Human Resources
c/o Human Resources
400 La Crosse Street
La Crosse, WI 54601
(608) 789-7595

Contact Person:
Employee Benefits Coordinator
c/o Human Resources
400 La Crosse Street
La Crosse, WI 54601
(608) 789-8310

II. Workforce Training

It is the Employer's policy to train all members of its workforce on its privacy policies and procedures. The Privacy Official is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within the Plan in compliance with HIPAA.

III. Administrative, Technical and Physical Safeguards and Firewall

The Employer will establish on behalf of the Plan appropriate administrative, technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

IV. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Plan;
- the individual's rights under the HIPAA privacy rules;
- the Plan's legal duties with respect to the PHI; and
- other information as required by the HIPAA privacy rules.

The privacy notice will inform participants that the Employer will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the Employer's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- no later than November 1st;
- on an ongoing basis, at the time of an individual's enrollment in the Plan or, in the case of providers, at the time of treatment and consent; and
- within 60 days after a material change to the notice.

The Plan will also provide notice of availability of the privacy notice (or a copy of the privacy notice) at least once every three years in compliance with the HIPAA privacy regulations.

V. Complaints

The Privacy Officer will be the Plan's contact person for receiving complaints.

The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with the Employer's discipline policy, up to and including termination.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of HIPAA or the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a disclosure of protected health information, either by an employee or a business associate the employee or the business associate, that is not in compliance with this policy or HIPAA, the employee should immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

VIII. 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 HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility under the Plan.

IX. Plan Documents

Plan documents shall include provisions to describe the permitted and required uses and disclosures of PHI by the Employer for plan administrative purposes or other permitted purposes. Specifically, Plan documents shall require the Employer to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Employer;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan;
- report to the privacy Officer any use or disclosure of the information that is inconsistent with the permitted use or disclosure and, if necessary, report such use or disclosure to the Department of Health and Human Services (HHS),as required by HITECH;
- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with HIPAA privacy rules;

- make the Employer's internal practices and records relating to the use and disclosure of PHI received from the Plan available to HHS upon request; and

- if feasible, return or destroy all PHI received from the Plan that the Employer still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

The Plan documents must also require the Employer to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the Employer agree to those restrictions; and (2) provide adequate firewalls in compliance with the HIPAA privacy rules.

X. Documentation

The Plan's privacy policies and procedures shall be documented and maintained for at least six years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must promptly be documented.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The Plan must maintain such documentation for at least six years.

Policies on Use and Disclosure of PHI

I. Use and Disclosure Defined

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

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the benefits department of the Employer, or by a Business Associate (defined below) of the Plan.

- *Disclosure.* For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Human Resources Department of the Employer, or not a Business Associate (defined below) of the Plan.

II. Workforce Must Comply With Plan's Policy and Procedures

All members of the Employer's workforce (described at the beginning of this Policy and referred to herein as "employees") who has access to Plan PHI must comply with this Policy and with the Plan's more detailed use and disclosure procedures, which are set forth in a separate document.

III. Access to PHI Is Limited to Certain Employees

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

- Any employee who performs functions directly on behalf of the Plan; and

- Department of Human Resources who has access to PHI on behalf of the Business Associate for its use in "plan administrative functions" of the covered entities.

The same employees may be named or described in both of these two categories. 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 (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and any associated procedures.

IV. Permitted Uses and Disclosures for Plan Administration Purposes

The Plan may disclose to the Employer for its use the following: (a) de-identified health information relating to plan participants; (b) Plan enrollment information; (c) summary health information for the purposes of obtaining premium bids for providing health insurance coverage under the Plan or for modifying, amending, or terminating the Plan; or (d) PHI pursuant to an authorization from the individual whose PHI is disclosed.

The Plan may disclose PHI to the following employees who have access to use and disclose PHI to perform functions on behalf of the Plan or to perform plan administrative functions ("employees with access"):

- Any employee who performs functions directly on behalf of the Plan; and
- Any other employee who has access to PHI on behalf of the Employer for its use in "plan administrative functions."

The same employees may be named or described in both of these two categories. 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 (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the more detailed use and disclosure procedures.

V. Permitted Uses and Disclosures: Payment and Health Care Operations

The Plan may disclose to the Employer for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

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:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;

- risk adjusting based on enrollee status and demographic characteristics;

- 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; and

- any other payment activity permitted by the HIPAA privacy regulations.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity 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 participant and the PHI requested pertains to that relationship.

Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development; and
- business management and general administrative activities; and
- any other payment activity permitted by the HIPAA privacy regulations.

VI. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Employer's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

VII. Mandatory Disclosures of PHI: to Individual and HHS

A participant's PHI must be disclosed as required by HIPAA in three situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows);
- The disclosure is required by law, or
- The disclosure is made to HHS for purposes of enforcing of HIPAA.

VIII. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The requirements include prior approval of the Employer's Privacy Official. Permitted are disclosures—

- about victims of abuse, neglect or domestic violence;
- for treatment purposes;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- for cadaveric organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

IX. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

X. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to HHS;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. The Plan, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All disclosures not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. The Plan, when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Plan is requested. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All requests not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

XI. Disclosures of PHI to Business Associates

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or

- 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.

XII. Disclosures of De-Identified Information

The Plan may freely use and disclose de-identified information in accordance with HIPAA privacy regulations. 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 ways a business associate can determine that information is de-identified: either by professional statistical analysis, or by removing specific identifiers.

XIII. Physical Access Controls/Guidelines to Guard PHI

The Employer will maintain strict physical access controls to its information systems at all times and under all conditions. This includes the physical security of electronic and paper data.

The Employer will terminate access to information systems and other sources of PHI, including access to rooms or buildings where PHI is located, when an employee, agent or contractor ends his/her employment or engagement. The Employer will terminate access to specific types of PHI when the status of any member of the workforce no longer requires access to those types of information.

Cleaning personnel:

Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets or rooms before cleaning personnel enter an area. When it is not reasonably possible to lock up PHI, it must be removed from sight before cleaning personnel enter an area and a supervisor must be present.

Computer Screens:

Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed. Computer displays will be configured to go blank, or to display a screen saver, when left unattended for more than a brief period of time. The period of time will be determined by the Compliance Official. Wherever practicable, reverting from the screen saver to the display of data will require a password. Computer screens left unattended for longer periods of time will log off the user. The period of time will be determined by the Privacy Official.

Compliance Official:

Director of Information Systems & Technology
City of La Crosse
400 La Crosse Street
La Crosse, WI 54601
(608) 789-8225

Conversations:

Conversations concerning individual care or other PHI must be conducted in a way that reduces the likelihood of being overheard by others. Wherever reasonably possible, barriers will be used to reduce the opportunity for conversations to be overheard.

Copying medical records and other PHI:

When PHI is copied, only the information that is necessary to accomplish the purpose for which the copy is being made, may be copied. This may require that part of a page be masked.

Desks and countertops:

Provider reports and other documents which may display identifiers and other "keys" to information should be placed face down on counters, desks, and other places where individuals or visitors can see them. Wherever it is reasonably possible to do so, medical reports and other documents containing PHI will not be left on desks and countertops after business hours. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers or other means to secure PHI during periods when the area is left unattended. In areas where locked storage after hours cannot reasonably be accomplished, PHI must be kept out of sight. A supervisor must be present whenever someone who is not authorized to have access to that data is in the area.

Disposal of paper with PHI:

Paper documents containing PHI must be shredded when no longer needed. If retained for a commercial shredder, they must be kept in a locked bin.

Home office:

Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures regarding the security and privacy of PHI, including these guidelines.

Key policy:

The Privacy Official will develop a list of which personnel, by job title, may have access to which keys. This includes keys to storage cabinets, storage rooms and buildings. All keys must be signed out. Keys must be surrendered upon termination of employment. The Privacy Official will ensure that locks are changed whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense.

Personal digital assistants (PDAs):

The privacy and security policies apply to any PHI that is stored on a PDA or laptop. Users of PDAs and laptops are responsible for assuring that the PHI on their devices is kept secure and private. Any loss or theft of a PDA or laptop thought to contain PHI must be reported to the Compliance Official immediately. Users of PDAs who store PHI on their devices will receive special training in the risks of this practice, and measures that they can take to reduce the risks (such as use of passwords).

Printers and Fax Machines:

Printers and fax machines must be located in secure areas, where only authorized members of the workforce can have access to documents being printed.

Records carried from one building to another:

When PHI is carried from one building to another, it must be signed out and signed in. When a member of the workforce is transporting PHI from one building to another, it may not be left unattended unless it is in a locked vehicle, in an opaque, locked container. Locking the vehicle alone is not sufficient.

Record Storage:

Areas where records and other documents that contain PHI are stored must be secure. Wherever reasonably possible, the PHI will be stored in locking cabinets. Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves and no unauthorized personnel may be left alone in such areas without supervision.

Workforce Vigilance:

All members of the workforce are responsible for watching for unauthorized use or disclosure of PHI, to act to prevent the action, and to report suspected breaches of privacy and security policies to their supervisor, or to the Privacy Official (example of a breach: individual or visitor looking through PHI left on a counter).

Visitors:

Visitors to areas where PHI is being used must be accompanied by a member of the Employer's workforce.

XIV. Breach Notification Requirements

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

Policies on Individual Rights

I. Access to PHI and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

Designated Record Set is a group of records maintained by or for the Plan that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or

- other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the patient's care or other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- as part of a limited data set;
- for specific national security or law enforcement purposes; or
- disclosures that occurred prior to the compliance date.

The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for subsequent accountings.

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the Employer, the requests are reasonable.

However, the Employer shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

IV. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Plan's' policy to attempt to honor such requests if, in the sole discretion of the Employer, the requests are reasonable. The Plan is charged with responsibility for administering requests for restrictions and shall communicate any restrictions to the
Privacy Official.

HIPAA PRIVACY USE AND DISCLOSURE PROCEDURES

Introduction

City of La Crosse (the "Employer") sponsors the following health plans:

- City of La Crosse Self-Funded Medical Benefit Plan (Two networks administered by Gundersen Lutheran Health Plan & Custom Benefit Administrators)

- City of La Crosse Section 125 Cafeteria Plan

For purposes of these procedures the plans listed above are referred to collectively and singularly as the "Plan." Members of the Employer's workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the Employer, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Employer's ability to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment

for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

It is the Employer's policy to comply fully with HIPAA's requirements. To that end, all members of the Employer's workforce who have access to PHI must comply with these Use and Disclosure Procedures. For purposes of these Use and Disclosure Procedures and the Employer's separate privacy policy, the Employer's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Employer, whether or not they are paid by the Employer. The term "employee" includes all of these types of workers.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by these Use and Disclosure Procedures. The Employer reserves the right to amend or change these Use and Disclosure Procedures at any time (and even retroactively) without notice. To the extent these Use and Disclosure Procedures establish requirements and obligations above and beyond those required by HIPAA, these Use and Disclosure Procedures shall be aspirational and shall not be binding upon the Employer. These Use and Disclosure Procedures do not address requirements under other federal laws or under state laws.

Procedures for Use and Disclosure of PHI

I. Use and Disclosure Defined

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

- Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the human resources department of the Employer, or by a Business Associate (defined below) of the Plan.

- Disclosure. For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the human resources department of the location(s) of the Employer.

II. Workforce Must Comply With Employer's Policy and Procedures

All members of the Employer's workforce (described at the beginning of these Use and Disclosure Procedures and referred to herein as "employees") must comply with these Use and Disclosure Procedures and the Employer's separate privacy policy.

III. Access to PHI Is Limited to Certain Employees

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

- Those employees who perform functions directly on behalf of the Plan, and

- Any other employee who has access to PHI on behalf of the Employer for its use in "plan administrative functions".

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 (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) except in accordance with these Use and Disclosure Procedures.

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

Definitions

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:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- 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.

Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development; and
- business management and general administrative activities.

Procedure

- 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.
- Disclosures must comply with the "Minimum-Necessary" Standard. (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation

Requirements."

- 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. These disclosures will be made according to procedures developed by the Privacy Official.

- 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. Such disclosures are made according to procedures developed by the Privacy Official.

- The disclosure must be approved by the Privacy Official.

- Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in "Disclosures Pursuant to an Authorization") has been received, an employee may not use a participant's PHI for the payment or operations of the Employer's "non-health" benefits (e.g., disability, worker's compensation, and life insurance). If an employee requires a participant's PHI for the payment or health care operations of non-Plan benefits, follow the steps provided by the Privacy Official.

- Obtain an Authorization. First, contact the Privacy Official to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, request an appropriate form from the Privacy Official. **Employees shall not attempt to draft authorization forms.** All authorizations for use or disclosure for non-Plan purposes must be on a form provided by (or approved by) the Privacy Official.

- Questions? Any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Official or his or her designated representative.

V. Mandatory Disclosures of PHI: to Individuals and HHS

Procedure

- Request From Individual. Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI, the employee must follow the procedure for "Disclosures to Individuals Under Right to Access Own PHI."

- Request From HHS. Upon receiving a request from a HHS official for disclosure of PHI, the employee must take the steps established by the Privacy Official.

- Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

VI. Permissive Disclosures of PHI: for Legal and Public Policy Purpose

Procedure

- Disclosures for Legal or Public Policy Purposes. An employee who receives 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" must contact the Privacy Official. Disclosures may be made according to procedures established by the Privacy Official.

- The disclosure must be approved by the Privacy Official.

- Disclosures must comply with the "Minimum-Necessary Standard."

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Legal and Public Policy Disclosures Covered

- Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:

    - The individual agrees with the disclosure; or

    - 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 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.

- For Judicial and Administrative Proceedings, in response to:

    - An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); and

    - 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.

- To a Law Enforcement Official for Law Enforcement Purposes, under the following conditions:

    - 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.

    - Information requested is limited information to identify or locate a suspect,

fugitive, material witness or missing person.

- Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.

- Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.

- Information that constitutes evidence of criminal conduct that occurred on the Employer's premises.

- To Appropriate Public Health Authorities for Public Health Activities.

- To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

- 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.

- 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.

- For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

- 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.

- For Specialized Government Functions, including disclosures of an inmate’s PHI to correctional institutions and disclosures of an individual's PHI to an authorized federal Official for the conduct of national security activities.

- For Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

VII. Disclosures of PHI Pursuant to an Authorization

Procedure

Disclosure Pursuant to Individual 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 Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

- Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Verify that the authorization form is valid. Valid authorization forms are those that:

  - Are properly signed and dated by the individual or the individual's representative;

  - Are not expired or revoked [the expiration date of the authorization form must be a specific date (such as July 1, 2010) 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)];

  - Contain a description of the information to be used or disclosed;

  - Contain the name of the entity or person authorized to use or disclose the PHI;

  - Contain the name of the recipient of the use or disclosure;

  - Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and

  - Contain a statement regarding the possibility for a subsequent re-disclosure of the information.

- All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

VIII. Disclosure of PHI to Business Associates

Definition of Business Associate

Business Associate is an entity or person who:

- performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration; data analysis, underwriting, etc.); or
- 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.

Procedure

Use and Disclosure of PHI by Business Associate. 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 Official and verify that a business associate contract is in place.

The following additional procedures must be satisfied:

- Disclosures must be consistent with the terms of the business associate contract.

- Disclosures must comply with the "Minimum-Necessary Standard." (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 Official.)

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

IX. Requests for Disclosure of PHI From Spouses, Family Members, and Friends

The Plan and Employer will not disclose PHI to family or 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.

- If an employee receives a request for disclosure of an individual's PHI from a spouse, family member or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."

- Once the identity of a parent or personal representative is verified, then follow the procedure for "Request for Individual Access."

- All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures Pursuant to Individual Authorization."

X. Disclosures of De-Identified Information

Definition of De-Identified Information

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 ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

Procedure

- Obtain approval from the Privacy Official for the disclosure. The Privacy Official will

verify that the information is de-identified.

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

XI. Verification of Identity of Those Requesting Protected Health Information

Verifying Identity and Authority of Requesting Party. Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such 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, a personal representative, or a public official seeking access.

- Request Made by Individual. When an individual requests access to his or her own PHI, the following steps should be followed:
  - Request a form of identification from the individual. Employees may rely on a valid driver's license, passport or other photo identification issued by a government agency.
  - Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.
  - Make a copy of the identification provided by the individual and file it with the individual's designated record set.
  - If the individual requests PHI over the telephone, ask for his or her social Security number.
  - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."
- 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:
  - 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.
  - Disclosures must be documented in accordance with the procedure "Documentation Requirements."
- Request Made by Personal Representative. When a personal representative requests access to an individual's PHI, the following steps should be followed:
  - Require a copy of a valid power of attorney or other documentation—requirements may vary state-by-state. If there are any questions about the validity of this document, seek review by the Privacy Official.

- Make a copy of the documentation provided and file it with the individual's designated record set.

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

- 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 "Mandatory Disclosures of PHI" or "Permissive Disclosures of PHI," the following steps should be followed to verify the official's identity and authority:

    - 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.

    - If the request is in writing, verify that the request is on the appropriate government letterhead.

    - 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 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.

    - 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. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Legal Department.

    - Obtain approval for the disclosure from the Privacy Official.

    - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

XII. Complying With the "Minimum-Necessary" Standard

Procedures for Disclosures

- Identify recurring disclosures. For each recurring disclosure, identify the types of PHI to be disclosed, the types of person who may receive the PHI, the conditions that would apply to such access, and the standards for disclosures to routinely-hired types of business associates. Create a policy for each specific recurring disclosure that limits the amount disclosed to the minimum amount necessary to accomplish the purpose of the disclosure.

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

Procedures for Requests

- Identify recurring requests. For each recurring request, identify the information that is necessary for the purpose of the requested disclosure and create a policy that limits each request to the minimum amount necessary to accomplish the purpose of the disclosure.

- For all other requests for PHI, contact the Privacy Official, who will ensure the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Exceptions

- The "minimum-necessary" standard does not apply to any of the following:
    - Uses or disclosures made to the individual;
    - Uses or disclosures made pursuant to an individual authorization;
    - Disclosures made to HHS;
    - Uses or disclosures required by law; and
    - Uses or disclosures required to comply with HIPAA.

XII. Documentation

Procedure

- Documentation. Employees shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued to participants;
- Copies of policies and procedures;
- Individual authorizations;
- When disclosure of certain PHI is made:
    - the date of the disclosure;
    - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
    - a brief description of the PHI disclosed;
    - a brief statement of the purpose of the disclosure; and
    - any other documentation required under these Use and Disclosure Procedures.

Note: The retention requirement only applies to documentation required by HIPAA. It does not apply to all medical records.

XIII. Mitigation of Inadvertent Disclosures of PHI

Mitigation: Reporting Required. HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. As a result, if you become aware of a disclosure of PHI, either by an employee of Plan or an outside consultant/contractor, that is not in compliance with the policies and procedures set forth in this manual, immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the individual can be taken.

XIV. Breach Notification Requirements

Compliance. The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

Procedures for Complying With Individual Rights

Individual Rights: HIPAA gives individuals the right to access and obtain copies of their protected health information that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that individuals may request to have their PHI amended, and that they are entitled to an accounting of certain types of disclosures.

I. Individual's Request for Access

"Designated Record Set" Defined

Designated Record Set is a group of records maintained by or for the Employer that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Review the disclosure request to determine whether the PHI requested is held in the individual's designated record set. See the Privacy Official 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 Official.

- 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, information compiled during research when the individual has agree 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 Official if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Official.

- 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 Employer will respond.

- A Denial Notice must contain (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) 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 Official.

- 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 (including inmates) also have the right to come in and inspect the information.

    - 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.

    - Charge a reasonable cost-based fee for copying, postage, and preparing a summary (but the fee for a summary must be agreed to in advance by the individual). This provision is not needed if the plan will not charge a fee.

    - Disclosures must be documented in accordance with the procedure "Documentation Requirements."

II. Individual's Request for Amendment

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a designated record set, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Review the disclosure request to determine whether the PHI at issue is held in the individual's designated record set. See the Privacy Official 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 Official.

- Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above). See the Privacy Official if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Official**.**

- Review the request for amendment to determine whether the amendment is appropriate—that is, determine whether the information in the designated record set is accurate and complete without the amendment.

- 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 Employer will respond.

- 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 unconnected information to the detriment of the individual.

- When an amendment request is denied, the following procedures apply:

    - All notices of denial must be prepared or approved by the Privacy Official. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) 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 (4) a statement of how the individual may file a complaint concerning the denial.

    - 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

Employer'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.

III. Processing Requests for an Accounting of Disclosures of Protected Health Information

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- 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.

- 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 Employer will respond.

- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by 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 April 14, 2004. The accounting does not have to include disclosures made:

- to carry out treatment, payment and health care operations;

- to the individual about his or her own PHI;

- incident to an otherwise permitted use or disclosure;

- pursuant to an individual authorization;

- for specific national security or intelligence purposes;

    - to correctional institutions or law enforcement when the disclosure was permitted

without an authorization; and

- as part of a limited data set.

- If any business associate of the Plan has the authority to disclose the individual's PHI, then Privacy Officer shall contact business associate to obtain an accounting of the business associate's disclosures.

- The accounting must include the following information for each reportable disclosure of the individual's PHI:

- the date of disclosure;

- the name (and if known, the address) of the entity or person to whom the information was disclosed;

- a brief description of the PHI disclosed; and

- 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.)

- 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 Official for more guidance.

- Accountings must be documented in accordance with the procedure for "Documentation Requirements."

IV. Processing Requests for Confidential Communications

Procedure

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- 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.

- The employee should take steps to honor requests.

- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

- All confidential communication requests that are approved must be tracked.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

V. Processing Requests for Restrictions on Uses and Disclosures of Protected Health Information

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for access to an individual's PHI, the employee must take the following steps: Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- The employee should take steps to honor requests.

- If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

- All requests for limitations on use or disclosure of PHI that are approved must be tracked.

- All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions.

Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements."

10/2019