

**Northeast Community College
Health Insurance Portability and Accountability Act
Privacy Use and Disclosure Plan**

Introduction

Northeast Community College (the College) sponsors and administers a group health plan (the Plan). Members of the College'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 College, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Company'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 College's policy to comply fully with HIPAA's requirements. To that end, all members of the College's workforce who have access to PHI must comply with these Use and Disclose Procedures. For purposes of the Use and Disclosure Procedures and the College's Privacy Policy, the College'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 College, whether or not they are paid by the College. 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 College 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 aspiration and shall not be binding upon the College. These Use and Disclosure Procedures do not address requirements under other federal laws or under state laws.

How These Use and Disclosure Procedures Are Organized: These Use and Disclosure Procedures include two Parts.

"Procedures for Use and Disclosure of PHI" includes the use and disclosure procedures that must be followed when PHI will be used or disclosed for the Plan's own payment and health care operations purposes and when PHI will be disclosed to third parties (but not the individual).

"Procedures for Complying With Individual Rights" includes procedures for complying with an individual's right to access, amendment, and accounting of PHI held in a designated record set. This section also includes procedures for addressing individual requests for confidential communications and for limits on use and disclosure.

Procedures for Use and Disclosure of PHI

I. Use and Disclosure Defined

The College 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 or accounting departments of the College, 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 or accounting departments of the College.

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

All members of the College'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 College's Privacy Policy.

The President shall designate a Privacy Official. This individual shall be responsible for the general administration of this Plan. The Privacy Official is presently the Director of Human Resources.

III. Access to PHI Is Limited to Certain Employees

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

- Human Resources Director, Executive Assistant, Administrative Assistant, Payroll Specialists, Director of Accounting, Dean of Administrative Services, Vice President of Administrative Services, Accounts Payable Specialists, Purchasing Specialist, Accounting Specialist, Cashier, Part-Time Cashier, Communications Assistant, Student Accounts Specialist, Programmer/Analysts, Computer Support/Email Specialist, Director of Information Services, and On-line Application Specialist.

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 with these Use and Disclosure Procedures.

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

Objective: Facilitate use or disclosure of PHI for payment purposes and health care operations under circumstances permitted by HIPAA.

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 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 and flex plan performances;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development; and
- business management and general administrative activities.

Procedures

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." (page 8) (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." (page 8)

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 entity's payment activities. Disclosures may be made under the following procedures:

- Disclosures must comply with the "Minimum-Necessary Standard." (page 8) (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." (page 8)

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 Company's "non-health" benefit (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 these steps:

- 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.
- 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." (page 8)

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.

V. Mandatory Disclosures of PHI: to Individuals and the Department of Health and Human Services (DHHS)

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." (page 7)

Request From DHHS. Upon receiving a request from a DHHS official for disclosure of PHI, the employee must take the following steps:

- Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information." (page 6)
- Disclosures must be documented in accordance with the procedures for "Documentation Requirements." (page 8)

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

Procedure

Disclosure 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 under the following procedures:

- The disclosure must be approved by the Privacy Official.
- Disclosures must comply with the "Minimum-Necessary Standard." (page 8)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements." (page 8)

Legal and Public Policy Disclosures Covered

For Judicial and Administrative Proceedings, in response to:

- An order of a court or an 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.

VII. Disclosures of PHI Pursuant to an Authorization

Objective: Facilitate disclosures of PHI as permitted by HIPAA when authorized by the individual whose PHI will be disclosed. PHI disclosed pursuant to an individual authorization may be disclosed for any purpose so long as the disclosure is consistent with the terms of the authorization.

Procedures

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." (page 6)

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;
- 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." (page 8)

VIII. Disclosure of PHI to Business Associates

Objective: Verify that disclosure of PHI to business associates is consistent with a valid business associate contract.

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.

Procedures

Use and Disclose 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." (page 8)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements." (page 8)

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

Objective: Protect privacy of individual's PHI by disclosing it only as authorized.

The Plan and College 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.

- If an employee receives a request for disclosure of an individual's PHI from a spouse, family member, or personal friend on 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 Identify of Those Requesting Protected Health Information." (page 6)
- Once the identity of a parent or personal representative is verified, then follow the procedure for "Request for Individual Access." (page 9)
- 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." (page 7)

X. Disclosure of De-Identified Information

Objective: Permit disclosure of de-identified information in accordance with HIPAA.

Definition of De-Identified Information

De-identified information in 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.

Procedures

- Obtain approval from 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

Objective: Verify identity and authority of individual requesting access to PHI.

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 drivers 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.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements." (page 8)

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." (page 8)

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. 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." (page 8)

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 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 Human Resources Office.
- Obtain approval for the disclosure from the Privacy Official.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements." (page 8)

XII. Complying With the "Minimum-Necessary" Standard

Objective: Limit the PHI used, disclosed or requested to the "minimum necessary" to accomplish the purpose of the use, disclosure or request, unless an exception applies.

Procedures for Disclosures

- Disclosures of PHI will be limited to the following purposes:
 - Enrollees in the group health plan and/or flexible benefit plan and the elected coverage and subsequent changes and terminations in election as required by business associates in administering the plans
 - De-identified information required in requesting bids for coverage of the above plans
- 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

- Requests for PHI relative to the group health plan and/or flexible benefit plan will be handled through the human resources or accounting departments of the College. The PHI released shall be limited to the name(s) and coverage amount elected in the group health plan, the employee name and coverage amount elected in the flexible benefit plan, and the de-identified information required in requesting bids for coverage of the above plans.
- For all other requests for PHI, contact the Privacy Official, who will ensure that 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 DHHS;
 - Uses or disclosures required by law; and
 - Uses or disclosures required to comply with HIPAA.

XIII. Documentation

Objective: Comply with the HIPAA mandate to document uses and disclosures of PHI.

Procedure

Documentation. Employer shall maintain copies of all 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.
- When a disclosure of 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.
- Individual authorizations.

XIV. 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.

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

Objective: To facilitate compliance with HIPAA's requirement to provide individuals with access to their own PHI.

"Designated Record Set" Defined

Designated Record Set is a group of records maintained by or for the Company 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, 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 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 College 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 (except for inmates) 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.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

II. Individual's Request for Amendment

Objective: To facilitate compliance with HIPAA's requirement to provide individuals with the right to request amendments to their own PHI.

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." (page 6)
- 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 College 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 uncorrected 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 College'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

Objective: To facilitate compliance with HIPAA's requirements to provide individuals with the right to receive an accounting of certain disclosures of their PHI.

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:

- Following 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." (page 6)
- 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.

- Record 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 Company 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. 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 the College will coordinate all requests with the business associates.
- 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.
- 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." (page 8)

IV. Processing Requests for Confidential Communications

Objective: Facilitate processing of 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 or Those Requesting Protected Health Information." (page 6)
- 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.

- 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 recorded in a separate file maintained by the Privacy Officer.
- 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

Objective: To facilitate the processing of requests for restrictions on uses and disclosures of PHI.

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."
- 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 approved and tracked by the Privacy Officer.
- 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." (page 8)