Loyola University New Orleans

HIPAA Privacy

Use and Disclosure

Policy and Procedures

Effective as Revised: January 1, 2016

Table of Contents

Introduction

1. Purpose

Loyola University New Orleans (the "University") sponsors a group health and welfare plan providing medical, dental, vision, prescription drug, employee assistance program, and health care flexible spending benefits (called the "Plan"), which is subject to the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and its implementing regulations, issued under the Privacy Regulations at 45 C.F.R. Parts 160 and 164 (the "Privacy Regulations"). The Plan and the University intend to comply fully with the Privacy Regulations' requirements. Thus, the University and the Plan establish this HIPAA Privacy Use and Disclosures Policy and Procedure (the "Policy"), effective as revised January 1, 2016.

Certain members of the University's workforce have access to Plan member's individually identifiable health information either (1) on behalf of the Plan itself; or (2) on behalf of the University, to perform administrative functions for the Plan. This Policy shall provide appropriate guidelines for members of the University's workforce who have access to Protected Health Information ("PHI").

Employees, volunteers, trainees, and other persons whose work performance is under the direct control of the University, whether or not they are paid by the University, are considered part of the University's workforce for purposes of this Policy.

2. No Third Party Rights

This Policy does not create any third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or Business Associates). The Policy shall be merely a guideline and shall not be binding upon the University to the extent this Policy establishes requirements and obligations above and beyond those required by the Privacy or Security Regulations. This Policy does not address requirements under other federal laws or under state laws.

3. Right to Amend without Notice

The University reserves the right to amend or change this Policy at any time (and even retroactively) without notice, except to the extent that notice is required by the Privacy Regulations.

4. Definitions

The terms used, but not otherwise defined in this Policy, shall have the same meaning as those terms are defined in the Privacy Regulations. The following definitions shall specifically apply:

Breach. A “breach” is the acquisition, access, or use or disclosure of unsecured protected health information in a manner not authorized by the HIPAA Privacy regulations which compromises the security or privacy of such information.

Business Associate. A 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, patient safety activities, etc.) or any other function or activity regulated by the Privacy Regulations on behalf of the Plan; or

- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, data transmission, or financial services, where the performance of such services involves giving the service provider access to PHI; or

- a subcontractor of a Business Associate, who performs functions for or provides services to a Business Associate on behalf of a covered entity, other than in the capacity of a member of the workforce of a Business Associate, and creates, receives, maintains, stores, or transmits PHI on behalf of a Business Associate.

See Appendix A for a list of Business Associates.

Covered Entity. A Covered Entity is a health plan, health care provider, or health care clearinghouse subject to the Privacy Regulations.

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: (1) professional statistical analysis conducted in accordance with the Privacy Regulations; or (2) removing 18 specific identifiers as outlined in the Privacy Regulations.

Designated Record Set. A Designated Record Set is a group of records maintained by or for the University 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.

Disclosure. Disclosure means any release, transfer, provision of access to, or divulging in any other manner of protected health information to persons not

authorized to act on behalf of the Plan (see the Section of this Policy titled "Limitations on Access to PHI" (page 10) for information on who is authorized to have access to PHI on behalf of the Plan).

ePHI. ePHI is any PHI that is covered under the Privacy and Security Regulations and is produced, saved, transferred, or received in electronic form.

Genetic Information. Genetic information means, with respect to any individual, information about: (1) that individual's genetic tests; (2) the individual's family members' genetic tests; (3) the manifestation of a disease or disorder in any of the individual's family members; and (4) any request for, or receipt of, genetic services or participation in clinical research which includes genetic services by the individual or any of the individual's family members. A family member is someone who is a first-degree, second-degree, third-degree, or fourth-degree relative of an individual, or someone who is a dependent of that individual. It also includes the individual's spouse.

HITECH Act. HITECH Act shall mean the Health Information Technology for Economic and Clinical Health Act contained in Public Law 111-5, as amended.

Plan. Plan means the Loyola University New Orleans Employee Benefit Plan providing medical, dental, vision, prescription drug, employee assistance program, and health FSA benefits.

Protected Health Information. Protected Health Information means information that:

(1) identifies an individual or for which there is a reasonable basis to believe the information can be used to identify the individual; and
(2) is created, maintained, or received by the Plan; and
(3) relates to**:**
    (a) the past, present, or future physical or mental health or condition of an individual;
    (b) the past, present, or future provision of health care to an individual; or
    (c) the past, present, or future payment for the provision of health care to an individual. Protected health information includes information of persons living or deceased (except that the Privacy and Security Rules do not protect the individually identifiable information of persons who have been deceased for more than 50 years).

Unsecured PHI. Unsecured PHI is PHI that is not secured through use of a technology or methodology identified by the Department of Health and Human Services as rendering the information unusable, unreadable, or indecipherable to unauthorized persons.

Use. Use means the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the University on behalf of the Plan, or by a Business Associate of the Plan.

Workforce Member. Workforce member means any individual who is an employee, volunteer, trainee, or other person whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not that individual is paid by the University.

Plan's General Policies

1. Plan's General Responsibilities

Under the Privacy Regulations, the Plan has certain obligations. Those obligations include the following:

- designating a HIPAA Privacy Officer;
- providing workforce training;
- creating physical and technical safeguards to protect PHI;
- creating internal policies and procedures;
- creating and distributing a Notice of Information Practices, or a Privacy Notice, and if needed, Breach Notifications;
- amending health plan documents;
- obtaining any needed Business Associate Agreements;
- responding to requests for access, copies, amendments to PHI, restrictions on use of PHI, confidential communication of PHI, and accounting of disclosures of PHI as required by the Privacy Regulations; and
- documenting compliance activity.

Set forth below are the guidelines the University will follow in order to meet these obligations.

2. Designation of the Privacy Officer

Donna Rochon will be the Privacy Officer for the Plan. The Privacy Officer will develop and implement the initial policies and procedures relating to privacy for the Plan and the University. The Privacy Officer will also receive questions, concerns, or complaints from Plan members under the Plan, about the privacy of their PHI. The Privacy Officer shall also periodically review applicable state law to determine the treatment of unemancipated minors for health care privacy purposes and review and revise guidelines as appropriate. The Privacy Officer may also designate certain Workforce Members to assist in the above functions.

In addition, the Privacy Officer will track uses and disclosures of PHI and respond to and track: (1) authorizations; (2) requests for an accounting of disclosures; (3) requests for inspection and copying; (4) requests to amend or correct PHI; (5) requests for restriction on use of PHI; and (6) requests for confidential communication of PHI. The Privacy Officer may also designate certain Workforce Members to assist in the above functions.

3. Workforce Training

The University will train all members of its workforce, who have access to PHI, on its privacy policies and procedures. The Privacy Officer will develop training schedules and programs so that all Workforce Members who have access to PHI

receive the training necessary and appropriate to permit them to carry out their functions within or on behalf of the Plan. New members of the workforce who have access to PHI will be trained within four weeks of joining the University. Subsequent training will occur promptly after any material change in these policies and procedures for Workforce Members affected by the material change, and all firewall Workforce Members shall undergo annual refresher training.

Workforce Members undergoing training on the University's privacy policies and procedures will be required to document their participation in training sessions. Documentation shall include the date of the training, the participant's name, and the participant's signature. The Privacy Officer shall keep a record of training sessions for six years from the date of training.

Firewall Workforce Members shall also be requested to sign a Confidentiality Agreement (Form "O") affirming their obligation to maintain the confidentiality of all Plan participants' PHI. The Privacy Officer shall maintain copies of Confidentiality Agreements for six years from the date of execution.

If a Workforce Member fails to undergo necessary training within the applicable timeframe, the Workforce Member will be reassigned to a position that does not require access to PHI, or appropriate corrective action (up to and including termination) may be taken.

4. Creation of Physical and Technical Safeguards to Protect PHI

The University has created appropriate physical and technical safeguards on behalf of the Plan to prevent PHI from intentionally or unintentionally being used or disclosed in violation of the Privacy Regulations. The current physical and technical safeguards are set forth in the Security Policies and Procedures section of this Policy (pages 52 – 59).

This Policy shall be reviewed and amended from time to time in order to maintain adequate and appropriate physical and technical safeguards.

5. Creation and Revision of Internal Policies and Procedures

The Plan shall create and maintain internal policies and procedures for the following:

- documenting use and disclosure of PHI as required by the Privacy Regulations;
- inspection and copying of PHI;
- amendment and correction of PHI;
- requesting restrictions on the use and disclosure of PHI;
- retention of records;
- revision of privacy policies and procedures;
- processing requests for accountings of use and disclosure of PHI;
- processing requests for confidential communications;
- handling authorizations;

- handling requests for use or disclosure of PHI;
- handling PHI related to unemancipated minors;
- handling disclosures about victims of abuse, neglect, or domestic violence;
- handling disclosures for judicial or administrative proceedings; and
- other policies and procedures as shall arise from time to time and are necessary to comply with applicable law.

Applicable policies and procedures shall be set forth in this Policy and amended from time to time as necessary to comply with applicable laws and regulations.

6. Creation of a Notice of Privacy Practices or Privacy Notice

The Privacy Officer has developed and will update and maintain a notice of the Plan's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Plan;
- an individual's rights under the Privacy Regulations;
- the Plan's obligations;
- the University's right to access PHI in connection with Plan administrative functions or on behalf of the Plan;
- the name, address, and telephone and fax numbers of the contact person for further information or for filing complaints; and
- the effective date of the notice.

The privacy notice will be individually delivered to all Plan participants:

- on an ongoing basis, at the time of the participant's enrollment in the Plan;
- upon request; and
- within 60 days after a material change to the notice.

At least every three years, the Plan will provide notice of availability of the privacy notice.

7. Amendment of the Plan Documents

Any applicable plan documents for the individual health and welfare plans comprising the Plan shall be amended to require the University to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that any agent or subcontractor to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the University;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan unless authorized to do so pursuant to a written authorization;

- report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to individuals who are the subject of the PHI, consider their amendments, and, upon request, provide them with an accounting of PHI disclosures as required by law;
- make the University's internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services ("HHS") upon request;
- if feasible, return or destroy all PHI received from the Plan that the University 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;
- establish separation between the Plan and the University in accordance with the requirements of the Privacy Regulations;
- implement administrative, physical, and technical safeguards that shall reasonably and appropriately protect the integrity, confidentiality, and availability of ePHI that the University creates, receives, maintains or transmits on behalf of the Plan;
- ensure that adequate and reasonable safety measures are in place to maintain the separation between the Plan and the University as described in 45 C.F.R. §164.504(f)(2)(iii);
- report to the Plan, at agreed upon times and frequency, the total number of unsuccessful, unauthorized attempts to use, access, disclose, modify, or destroy ePHI or to interfere with systems operations containing ePHI;
- report to the Plan any unsuccessful attempt to access, use, disclose, modify, or destroy ePHI or interfere with systems operations where ePHI is housed as soon as practicable; and
- ensure that any agent or subcontractor to whom the University provides ePHI received from the Plan agree to implement reasonable and appropriate safeguards to protect the ePHI.

The Plan document will also be amended to require the University to: (1) certify to the Plan that the Plan documents have been amended to include the above restrictions and that the University agrees to those restrictions; and (2) provide adequate safeguards against unintentional or intentional disclosure of PHI.

8. Documentation of Compliance Activity

The Plan and the University shall ensure that Plan documents are appropriately amended, that the Plan Sponsor Certification is in place, and that appropriate Business Associate Agreements are entered into and maintained. The Plan's and the University's privacy policies and procedures shall be documented and maintained for at least six years. Policies, procedures, forms, plan documents,

and Business Associate Agreements will be (1) changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations); and (2) reviewed at least once every three years. Any changes to policies, procedures, forms, plan documents, and Business Associate Agreements shall be promptly documented.

Any changes will be effective only with respect to PHI created or received after the date of notification to affected individuals of the change.

Limitations on Access to PHI

Access to Plan member's PHI shall be limited to the following University Workforce Members:

Vice Provost for IT and CIO	Director Information Management
Systems Specialist	Systems Analyst
Senior Programmer Analyst	IT Production Control Specialist
VP Finance/Administration	Associate VP Financial Affairs
Internal Auditor	Director Human Resources
HR Generalist/Representative	Manager – Payroll and Benefits
Benefits Specialist	Payroll Administrator
HR Coordinator	Senior Accountant
Director of Risk Management	Administrative Assistant for HR
President	Budget Manager
Sr. Information Analyst	Coordinator Information Reporting
Research/Assessment Associate	Controller – Operations

These Workforce Members shall be referred to as "Workforce Members with access" or "firewall Workforce Members." The firewall Workforce Members may use and disclose PHI for plan administrative functions. They may also disclose PHI to other firewall Workforce Members for plan administrative functions subject to the **"Minimum Necessary Standards"** addressed beginning on page 43. Firewall Workforce Members may not disclose PHI to Workforce Members (other than Workforce Members with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the Privacy Regulations.

Under certain circumstances, PHI will be shared with Workforce Members in the University's Legal Department and/or to internal or external auditors, consultants, or legal counsel who are bound by the terms of their University confidentiality agreements and/or professional codes of conduct. If outside auditors, consultants, or legal counsel are retained to assist the Plan or the University, and it is necessary to share PHI with those auditors, consultants, or legal counsel, the auditors, consultants, or legal counsel shall be required to sign a confidentiality agreement or a Business Associate Agreement, as appropriate, prior to receiving PHI.

Mandatory Use and Disclosure Policy and Procedures

1. Disclosures of PHI to an Individual: Requests to Inspect and Copy and Requests for Accounting of Disclosures

a. Policy

PHI must be disclosed to an individual, who is the subject of PHI, seeking access to his or her own PHI or requesting an accounting of certain PHI disclosures.

b. Procedure

When an individual requests disclosure of his or her own PHI through a request to inspect protected health information or a request for an accounting of certain disclosures, the following steps should be followed:

- Request identification from the individual. The individual may provide 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. Contact the Privacy Officer if any doubts arise as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI.

- Make a copy of the identification provided by the individual and file it with the individual's Designated Record Set.

- Request that the individual complete an **"Individual Request to Inspect Protected Health Information"** form (Form "C") or **"Individual Request for Accounting of Disclosures of Protected Health Information"** form (Form "K"), as applicable.

- The **"Individual Request to Inspect Protected Health Information"** or **"Individual Request for Accounting of Disclosures of Protected Health Information"** form should be completed and forwarded to the Privacy Officer for retention and any further necessary action.

- When responding to a request to inspect protected health information, complete the **"Response to Individual Request to Inspect Protected Health Information"** form (Form "D"). Provide the original response to the requesting individual and retain a copy in the individual's Designated Record Set. Provide access in the manner indicated on the Response form.

- When responding to a request for an accounting of disclosures of Protected Health Information, provide a copy of the **"Protected Health Information Disclosure"** form (Form "P") for each disclosure for which accounting is required. Original disclosure forms should be maintained in the individual's Designated Record Set.

- Determine if an accounting is required. If required, provide an accounting using Form P and keep a copy in the individual's Designated Record Set. See Form P for specific information regarding timing of disclosure and any applicable fees for providing an accounting.

- Retain all records for the applicable six year period.

2. Disclosures of PHI to the Department of Health and Human Services ("HHS")

a. Policy

PHI must be disclosed to the Department of Health and Human Services ("HHS") when required by HHS to determine Covered Entity's compliance with the Privacy Regulations. Such a disclosure is only required to enforce the Privacy Regulations, and not for other reasons (e.g., coordinating benefits under the Medicare Secondary Payer laws).

b. Procedure

Upon receiving a request from a HHS official for disclosure of PHI, take the following steps:

- Verify the identity of a public official following the procedures set forth in **"Verification of Identity of Those Requesting Protected Health Information"** on pages 41 – 42.

- Document disclosures in accordance with the **"Documentation Requirements"** beginning on page 49.

If a Workforce Member receives a subpoena or a similar request from a public agency, such as HHS, for the disclosure of PHI, it should be referred to the Privacy Officer for further handling.

Permissible Use and Disclosure Policy and Procedures

1. Uses and Disclosures for Purposes of Payment and Health Care Operations

a. Policy

PHI may be disclosed for the Plan's own payment and health care operations purposes, and PHI may be disclosed to another covered entity for the payment purposes or certain health care operations 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. Such activities must relate to the individual to whom health care is provided, not violate the prohibition against using genetic information in violation of the Genetic Information Nondiscrimination Act, and include (but will not be limited to):

- determination of eligibility;
- determination of coverage;
- determination of cost-sharing amounts;
- coordination of benefits;
- adjudication of health benefit claims (e.g. claim administration);
- subrogation of health benefit claims;
- risk adjusting amounts due based on enrollee status and demographic characteristics;
- billing, collection activities, and related health care data processing, including auditing payments, investigating and resolving payment disputes and responding to customer inquiries about payments;
- obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing;
- review of health care services with respect to medical necessity, or reviews of appropriateness of care or justification of charges;
- utilization review activities, including pre-certification of services, and concurrent or retrospective review of services; and
- disclosure to consumer reporting agencies related to the collection of premiums or reimbursement (the following PHI may be disclosed for payment purposes: name and address, date of birth, Social Security number, payment history, account number and name and address of the provider and/or health plan).

Health Care Operations. Health care operations mean any of the following activities to the extent that they are related to Plan administration or other Covered Functions:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and securing a contract for reinsurance of risk relating to claims for health care (including stop loss insurance and excess of loss insurance) provided that the requirements of the Privacy Regulations are met, if applicable, and no genetic information shall be used for purposes of underwriting except for use with any applicable long-term care policy;
- conducting or arranging for medical review, legal services and auditing functions, including, but not limited to, fraud and abuse detection and compliance activities;
- patient safety activities;
- business planning and development; and
- business management and general administrative activities of the Plan, including, but not limited to, customer services, resolving internal grievances, or the sale, transfer, merger, or consolidation of all or part of the Plan with another covered entity and due diligence related to such activity.

Payment or Health Care Operations of Another Covered Entity. PHI may be disclosed to another covered entity for purposes of the other covered entity's payment purposes such as for Coordination of Benefits or 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.

b. Procedure

(1) Uses and Disclosures for Plan's Own Payment Activities or Health Care Operations.

The Plan may use and disclose an individual's PHI to perform the Plan's own payment activities or health care operations. Disclosures must:

- comply with the **"Minimum-Necessary Standard"** (pages 43 – 47) (If the disclosure is not recurring, the disclosure must be approved by the Privacy Officer); and

- be documented in accordance with the **"Documentation Requirements"** (beginning on page 49).

(2) Disclosures for Another Covered Entity's Payment Activities or Certain Health Care Operations

The Plan may disclose an individual's PHI to another covered entity to perform the

other entity's payment activities. PHI may also be disclosed for purposes of another 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, who is the subject of the PHI, and the PHI requested pertains to that relationship. Disclosures must:

- comply with the **"Minimum-Necessary Standard"** (pages 43 – 47) (If the disclosure is not recurring, the disclosure must be approved by the Privacy Officer); and

- be documented in accordance with the procedure for **"Documentation Requirements"** (beginning on page 49).

2. Disclosures of PHI Pursuant to an Authorization

a. Policy

PHI may be disclosed for any purpose if an authorization that satisfies all of the Privacy Regulations' requirements for a valid authorization is provided by the individual, who is the subject of the PHI (or his or her designated personal representative or legal guardian). Any use or disclosure of PHI made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

The University and the Plan have an approved **"Authorization for Release of Health Information"** (Form "A"), which should be used whenever possible. The **"Authorization for Release of Health Information"** may be revoked at any time by an individual. (See Form "B.") Both authorizations and revocations shall be retained for the applicable six year period.

Unless the individual, who is the subject of the PHI (or his or her designated personal representative or legal guardian), provides an authorization to use or disclose PHI for non-health plan purposes (as discussed in **"Disclosures Pursuant to an Authorization"** below) or such use or disclosure is required by applicable state law and all applicable requirements under the Privacy Regulations are met, PHI may not be used or disclosed for the payment or operations of the University's "non-health" benefits as defined by HIPAA (e.g., disability, workers' compensation, life insurance, etc.).

b. Procedure

(1) Disclosures pursuant to an authorization

If disclosure pursuant to an authorization is requested, the following procedures should be followed:

- Verify the identity of the individual (or individual's personal representative) providing the authorization as set forth in **"Verification of Identity of Those Requesting Protected Health Information"** on pages 40 – 42.

- 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 31, 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), but in no event longer than permitted by applicable state law];
  - 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 PHI ;
  - 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.

- Follow the terms and conditions of the authorization.

- Document the disclosure in accordance with the procedure for **"Documentation Requirements"** beginning on page 49.

- Retain the Authorization (and any applicable Authorization Revocation) in the individual's Designated Record Set for the applicable six year period.

The University has an approved authorization for Plan participant's use. Where at all possible, the University's authorization should be used. (See Form "A.")

(2) Disclosure of PHI for Non-Health Plan Purposes

If the payment or health care operations of non-health benefits (e.g., short-term disability or life insurance) requires an individual's PHI, follow these steps:

- Contact the Privacy Officer to determine if an authorization for this type of use or disclosure is already on file.

- If no form is on file, request that the individual complete an authorization form. (See Form "A.") ***Workforce Members 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 Officer.

- Make any necessary disclosures according to the **"Minimum-Necessary Standard"** on pages 43 – 47.

- Document disclosures in accordance with the **"Documentation Requirements"** beginning on page 49.

- Retain all appropriate documents for the applicable six year period.

3. Disclosure of PHI to Business Associates

a. Policy

Employees may disclose PHI to the Plan's Business Associates and allow the Plan's Business Associates to create or receive PHI on behalf of the Plan. However, prior to disclosing PHI to a Business Associate or allowing a Business Associate to create or receive PHI on behalf of the Plan, the Plan must obtain written assurances, from the Business Associate through a contract or other agreement, that meet the applicable requirements of the Privacy and Security Regulations, that the Business Associate will appropriately safeguard the information. Before sharing PHI with outside organizations who meet the definition of a "Business Associate," contact the Privacy Officer and verify that a Business Associate contract is in place.

The Privacy Officer shall retain all Business Associate agreements for at least six (6) years after the date the applicable agreement is no longer in effect.

If the Plan learns that a Business Associate has materially violated the Business Associate agreement in place with the Plan, the Plan will notify the Business Associate of the material violation. The Plan may provide an opportunity for the Business Associate to cure the material breach, or the Plan may terminate the agreement between the parties, as governed by the applicable Business Associate Agreement between the Plan and the Business Associate. If the Plan determines that the material breach cannot be cured and that it is not feasible to terminate the agreement, the Plan must report the violation to HHS.

b. Procedure

(1) Disclosures to Business Associates

Before providing PHI to a Business Associate, Workforce Members must contact the Privacy Officer and verify that a Business Associate contract is in place. The following additional steps must be taken:

- Disclosures must be consistent with the terms of the Business Associate contract.

- Disclosures must comply with the **"Minimum-Necessary Standard"** on pages 43 – 47. Recurring disclosures will be subject to the minimum-necessary standards set forth below, and each non-recurring disclosure must be approved by the Privacy Officer.

- Document disclosures, if necessary, in accordance with the **"Documentation Requirements"** beginning on page 49.

(2) Material Breach of Business Associate Agreement

If a Plan representative learns of a material breach of a Business Associate agreement, the representative shall notify the Privacy Officer as soon as practicable. The Privacy Officer will inform the Business Associate of the material breach and of any opportunity to cure. If the Business Associate does not satisfactorily cure the breach (in the professional judgment of the Privacy Officer), the Privacy Officer will notify (in writing) the Business Associate of immediate termination of the Business Associate agreement. If the Plan determines that the Business Associate agreement cannot be terminated despite the failure to cure a material breach, the Privacy Officer will notify HHS of the material breach.

Documentation and correspondence related to a material breach of a Business Associate agreement shall be retained for six (6) years following the date the breach was discovered, the agreement was terminated, or the notice was sent to HHS, whichever is latest. If termination is not feasible, the Privacy Officer will document notification to HHS and the reason or reasons why termination is not feasible.

4. Disclosures of PHI for Legal and Public Policy Purposes

a. Policy

PHI may be disclosed in the following situations without an individual's authorization, when specific requirements are satisfied. Permitted disclosures are disclosures:

- about victims of abuse, neglect or domestic violence;
- 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 public health or safety;

- for specialized government functions; and
- to the extent necessary to comply with laws relating to workers' compensation programs.

b. Procedure

Before making a permissible disclosure of PHI for legal and public policy purposes, take the following steps:

- Notify and obtain approval for the disclosure from the Privacy Officer.

- Provide information in accordance with the **"Minimum-Necessary Standard"** on pages 43 – 47.

- Document the disclosure in accordance with the **"Documentation Requirements"** beginning on page 49.

- Make sure that the following specific requirements set forth below have been met:

(1) Disclosures about victims of abuse, neglect or domestic violence

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

- The individual, who is the subject of the PHI, agrees with the disclosure; or

- A statue or regulation expressly authorizes the disclosure, and the disclosure prevents harm to the individual (or other victim) or the individual, who is the subject of the PHI, is incapacitated and unable to agree, and the information will not be used against the individual and is necessary for an imminent enforcement activity. The individual must be promptly informed of the disclosure unless prompt notification would place the individual at risk or if informing the individual would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

Contact the Privacy Officer for a determination as to whether the disclosure concerns a victim of abuse, neglect, or domestic violence.

(2) For Judicial and Administrative Proceedings

Disclosure for purposes of judicial and administrative proceedings may be made if the following conditions are met:

- The Plan receives a court or administrative order; or

- The Plan receives a subpoena, discovery request or other lawful process, not accompanied by a court or administrative order, which meets the standards set forth below:

(a) Court or Administrative Order

If the Plan receives a court or administrative order, the following steps should be taken:

- Verify that the order is made by a court or an administrative agency.
- Release only the PHI expressly authorized by the order.

(b) Subpoena, discovery request, or other lawful process

If the Plan receives a subpoena, discovery request, or other lawful process without a court or administrative order, the following steps should be taken:

- Obtain satisfactory assurance from the party seeking the information that either of the following have occurred:
  - The individual who is the subject of the request has been notified of the request, or
  - The party seeking the information has obtained a qualified protective order that meets the requirements of the Privacy Regulations.

A "qualified protective order" is a court or administrative agency order that: (1) prohibits the parties from using or disclosing PHI for any purpose other than use in the litigation or proceeding for which the PHI is requested; and (2) requires the PHI to be returned to the Plan or destroyed at the end of the litigation or proceeding.

Satisfactory assurance that the party seeking the information has notified the individual who is the subject of the request can be met by the following statements from the party seeking the information:

- The party seeking the disclosure made a good faith effort to provide written notice to the individual, who is the subject of the PHI, or, if that individual's location is unknown, that the party mailed a notice to that individual's last known address;
- The notice contained sufficient information about the litigation or proceeding for which the PHI is sought to allow the individual to object to the court or administrative agency; and
- The time allowed for the individual to raise objections to the court or administrative agency has passed, and objections were either not filed, or

any objections were resolved by the court or administrative agency in a manner permitting the disclosures.

Satisfactory assurance that a qualified protective order exists may be met by receipt of a copy of an agreed qualified protective order or a qualified protective order signed by the appropriate court or administrative agency.

If the satisfactory assurances identified above are not met, the Plan will consult legal counsel for advice.

(3) To a Law Enforcement Official for Law Enforcement Purposes

Disclosures to law enforcement officials or for law enforcement purposes may be made 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 about a deceased individual upon suspicion that the individual's death resulted from criminal conduct, but only to alert law enforcement about the death.

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

- Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.

  - Information disclosed to identify or locate a suspect, fugitive, material witness or missing person must be limited to the following information:

    - Name and address;
    - Date and place of birth;
    - Social Security number;
    - ABO blood type and RH factor;
    - Type of injury;
    - Date and time of treatment;
    - Date and time of death, if applicable; and
    - A description of any distinguishing physical characteristics such as height, weight, gender, race, hair color, eye color, absence or presence of facial hair, scars, and tattoos.

- **Unless PHI is disclosed to a law enforcement official to identify or locate a suspect, fugitive, material witness or missing person, PHI may NOT be disclosed that is related to an individual's DNA or DNA analysis, dental records, blood type, samples, or analysis of body fluids or tissue.**

- 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, if disclosure is in the best interest of the individual, and if the individual cannot agree because of incapacity or another emergency.

  - Prior to releasing PHI to a law enforcement official about a suspected victim of a crime who has not agreed to the disclosure, the following steps must be taken:

    - Obtain a statement from the law enforcement official that the PHI is needed to determine whether a crime has occurred;

    - Obtain a statement from the law enforcement official that the PHI will not be used against the victim;

    - Obtain a statement from the law enforcement official that immediate law enforcement action depends on the PHI and would be materially and adversely affected by waiting for the individual to agree to the disclosure; and

    - Notify the Privacy Officer to determine whether the disclosure is in the individual's best interest in the professional judgment of the Plan.

  - The statement from the law enforcement official may be oral or written.

(4) To Appropriate Public Health Authorities for Public Health Activities to the extent permitted by the Privacy Regulations.

PHI may be disclosed to the appropriate public health authorities for public health activities as permitted by the Privacy Regulations. Contact the Privacy Officer for guidance.

(5) To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

PHI may be disclosed to a health oversight agency for health oversight activities if the following conditions are met:

- The requesting agency is an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory (including American Samoa and the Northern Mariana Islands), or an Indian Tribe (or a person or contractor acting upon its authority) that is authorized by law to oversee one of the following:

  - The public or private health care system;
  - A government program or programs in which health information is necessary to determine eligibility or compliance; or
  - A government program or programs to enforce civil rights laws for which health information is relevant.

- The PHI may only be used by the requesting agency for the following purposes:

  - Audits;
  - Civil or criminal investigations;
  - Inspections;
  - Licensure or disciplinary actions;
  - Civil, administrative, or criminal proceedings; or
  - Actions or other activities necessary for appropriate oversight of and by relevant agencies.

(6) To a Coroner or Medical Examiner About Decedents

PHI may be disclosed to a coroner or medical examiner to identify a deceased person, determine the cause of death, or for other duties as authorized by law. PHI may also be disclosed to a funeral director – under applicable state law – to allow the director to carry out duties related to the decedent.

(7) For Cadaveric Organ, Eye or Tissue Donation Purposes

PHI may be disclosed to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating organ, eye, or tissue donation or transplantation.

(8) For Certain Limited Research Purposes

PHI may be disclosed for certain limited research purposes provided that a waiver of the authorization required by the Privacy Regulations has been approved by an appropriate privacy board (as defined by Section 164.512(i)(1)(i) of the Privacy Regulations).

(9) Emergency Situations

PHI may be disclosed to avert a serious threat to health or safety of an individual 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.

(10) For Specialized Government Functions

PHI may be disclosed for specialized government functions, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials, for the conduct of national security activities.

(11) For Workers' Compensation Programs

PHI may be disclosed for purposes of administering workers’ compensation only to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

Policies and Procedures for Complying With Individual Rights

1. Request for Access (Inspection and Copying)

a. Policy

Individuals have the right to inspect and obtain copies of their PHI that the Plan (or its Business Associates) maintains in a **"**Designated Record Set.**"** "Designated Records Sets" are records containing PHI used to make decisions about individual members such as enrollment, claims adjudication, or case management information maintained by or for a group health plan about an individual. The Plan shall maintain Designated Record Sets for six years from the date of the record's creation or the date the record was last in effect, whichever is later. The Plan will provide access to PHI for requests that are submitted in writing. (See Form "C.")

The Plan and the University will not disclose PHI to family and friends of an individual except as required or permitted by the Privacy Regulations. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI. However, a guardian, an individual with a health care Power of Attorney, or another authorized personal representative (as defined under the Privacy Regulations) has the authority to invoke an individual's right to access (inspect and copy).

b. Procedure

Individuals seeking to inspect and copy PHI must complete a request form (see Form "C"). Workforce Members shall not create a Request to Inspect Protected Health Information form. Forms are available from the Privacy Officer.

(1) Request From Individual, Parent of Minor Child, or Personal Representative

If the Plan receives a written request to inspect and copy PHI from an individual (or from a minor child's parent or an individual's personal representative), take the following steps:

- Verify the individual's (or parent's or personal representative's) identity. (See **"Verification of Identity of Those Requesting Protected Health Information"** on pages 40 – 42.)

- If a minor child is involved, contact the Privacy Officer for guidance. Whether an individual is a minor child must be determined in accordance with the provisions of the applicable state law of the child's place of residence.

- After verifying the identity of a parent or personal representative, follow the procedure for **"Processing the Request for Access"** beginning on page 26.

(2) Requests From Spouse, Family Member or Friend

If the Plan receives a Request for disclosure from a spouse, family member, or friend, who is not a personal representative or the parent of a minor child, any use or disclosure must be authorized by the individual whose PHI is involved. See the procedures for **"Disclosures Pursuant to Authorization"** on page 15. An Authorization form is available from the Privacy Officer. (See Form "A.")

(3) Processing the Request

After verifying the identity of the requesting individual or obtaining the necessary authorization, take the following steps:

- Review the request to determine if the PHI requested is in the individual's Designated Record Set. See the Privacy Officer if it appears that the requested information is not in the individual's Designated Record Set. ***Only the Privacy Officer may deny a Request to Inspect Protected Health Information.***

- Submit the disclosure request to the Privacy Officer for a determination whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access any of the following:

  - 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 compiled for use in or in anticipation of a civil, criminal, or administrative proceeding;
  - the records are subject to the Privacy Act, 5 U.S.C.A. § 552a (government records);
  - information obtained under a promise of confidentiality; and
  - other disclosures that are determined by a health care professional to be likely to cause harm.

- Respond to the request by providing the information for inspection or copying or denying the request in writing within 30 days. Use the appropriate response form. (See Form "D.") All responses must be in

writing. A copy of the request and the response shall be maintained in the individual's HIPAA file for the appropriate six year period.

- If the requested PHI cannot be presented for inspection and copying within the 30-day period, the deadline may be extended for 30 days by providing written notice – using the appropriate form (Form "D") -- to the individual within the original 30-day period of the reasons for the extension and the date by which the University will respond.

- If no grounds exist to deny a request to inspect and copy, provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.

- Individuals have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals also have the right to come in and inspect the information. Individuals also have the right to request that PHI be sent directly to a third party, either electronically or in paper format. If PHI is to be delivered electronically, the email address must be verified prior to sending the PHI to the intended recipient. This may be accomplished by sending a request for a confirmation to the intended recipient. Reasonable safeguards shall be used to transmit PHI pursuant to the University's policy on transmission of PHI, beginning on page 55.

- If the Plan uses or maintains electronic protected health information in an electronic designated record set maintained by the Plan, individuals are entitled to copies of their protected health information in an electronic format, if it is readily producible, or if not, in a readable electronic form and format agreed to by the Plan and the individual. Individuals may direct the Plan to transmit a copy of the ePHI directly to a third party they designate clearly and specifically.

- If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, in a request to inspect and copy, 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.

- In response to a request to inspect and copy, the Plan may 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).

(4) Handling denials

If the Request for Inspection and Copying must be denied, take the following steps:

- Obtain approval for such action from the Privacy Officer.

- Provide a written denial (Form “D”).

- A denial 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 with the Secretary of Health and Human Services and the Plan concerning the denial. All denials must be prepared or approved by the Privacy Officer. Denial of a request to inspect and copy in inappropriate circumstances could lead to liability. For this reason, the Plan requires all denials to be approved by the Privacy Officer.

- If a Request to Inspect and Copy is denied, the requesting individual is entitled to a review of the denial if the access to PHI is denied on the basis of a “Reviewable Ground for Denial.”

  - A Reviewable Ground for Denial exists if one of the following conditions is met:

    - Access will reasonably likely endanger the life or physical safety of the individual who is the subject of the PHI; or

    - The PHI refers to another individual (except for a health care provider) and access will reasonably likely cause substantial harm to that other individual; or

    - The request for inspection and copying was made by the individual’s personal representative and access will be reasonably likely to endanger the life or physical safety of the individual or another person.

  - The individual must request a review in writing.

  - The review shall be promptly conducted by a “Designated Review Officer.” The Designated Review Officer shall be designated by the University and shall review the denial of access and render a decision as to whether access should be granted or denied. The Designated Review Officer must be a licensed health care processional who was not directly involved in the initial decision to deny access to the PHI. The Designated Review Officer may be named on a case-by-case basis.

(5) Documentation and Retention

- Document disclosures in accordance with the **"Documentation Requirements"** beginning on page 49.

- Retain appropriate documents for the applicable six year period.

2. Request for Amendment or Correction

a. Policy

Individuals also have the right to request that their PHI be amended or corrected. The Plan will consider written requests for amendment or correction. Forms to request amendments or correction are available from the Privacy Officer.

b. Procedure

Upon receiving a request for amendment or correction of PHI held in a Designated Record Set from an individual (or a minor's parent or an individual's personal representative), take the following steps:

- Verify the identity of the individual (or parent or personal representative) following the procedures set forth in "**Verification of Identity of Those Requesting Protected Health Information"** on pages 40 – 42.

- Obtain a copy of the personal representative's authority (e.g., health care Power of Attorney), if applicable, and file in the individual's Designated Record Set.

- Request that the individual complete the **"Individual Request to Amend or Correct"** form. (See Form "E.")

- Review the request for amendment or correction to determine whether the PHI at issue is held in the individual's Designated Record Set. See the Privacy Officer if it appears that the requested information is not held in the individual's Designated Record Set. ***No request for amendment or correction may be denied without approval from the Privacy Officer***.

- Review the request for amendment or correction to determine whether the information access can be denied under the Privacy Regulations' exceptions to the right to inspect and copy (see the request for inspection and copying procedures above). Contact the Privacy Officer if there is any question about whether one of these exceptions applies. ***No request for***

amendment or correction may be denied without approval from the Privacy Officer.

- Review the request for amendment or correction to determine whether the amendment or correction is appropriate – i.e., determine whether the information in the Designated Record Set is accurate and complete without the amendment or correction. If it is accurate and complete without the amendment or correction, the request may be denied.

- Respond to the request within 60 days by informing the individual in writing, using the **"Response to Request to Amend or Correct"** form (Form "F"), 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 University 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 Officer. A denial must be in writing and 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 with the Secretary of Health and Human Services and the Plan concerning the denial.

  - The plan may deny an individual's Request for Amendment, if the Privacy Officer determines the following:

    - The Request for Amendment relates to PHI that was not created or generated by the Plan. However, if the individual seeking the amendment gives a reasonable basis to show that the person or entity that created or generated the PHI is no longer available to respond to the Request for Amendment, then the Plan cannot deny the Request on the basis that the Plan did not create or generate the PHI.

- ❖ The Request for Amendment relates to PHI that is not part of the Designated Record Set.

- ❖ The Request for Amendment relates to PHI to which the requesting individual would not have access because the PHI falls into one of the categories for which no right to access exists or for which access may be denied.

- ❖ The Request for Amendment relates to PHI that is accurate and complete without amendment.

- If the request is denied, provide the individual with a **"Statement of Disagreement with Response to Request to Amend or Correct a Record"** (see Form "L").

- 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; and the University'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.

- Retain all applicable documents for the appropriate six year period.

3. Requests for an Accounting of Disclosures of PHI

a. Policy

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, or to an individual's personal representative, about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an individual authorization;
- as part of a limited data set;
- to correctional institutions or law enforcement officials when the disclosure was permitted without an authorization; or
- for national security or intelligence purposes.

The Plan must document and retain the following: (1) the date of a disclosure; (2) the name or entity or person who received the PHI and, if known, the address of the entity or person; (3) a brief description of the PHI disclosed; (4) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; (5) the written accounting provided to the individual; and (6), the titles of the persons or offices responsible for receiving and processing requests for an accounting by an individual. (See Form "P.") This information shall be retained by the University's Privacy Officer. The Plan is not required to track uses and disclosures of PHI made according to the Plan's ability to disclose information as long as, when possible, the individual who is the subject of the PHI has the opportunity to object, in the following circumstances:

- to family members or close friends for health care or payment purposes;
- to family members of close friends to notify, locate, or identify an individual and to provide information regarding an individual's general condition or death; or
- to public or private entities authorized to assist in disaster relief efforts.

The accounting must include the following information:

- 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).

The University and the Plan have provided a form (Form "P") allowing for collection of all appropriate information.

If an individual requests multiple disclosures to the same individual or entity, or if an individual requests that multiple disclosures be made under a single authorization, the Plan may make a summary entry. The summary entry will include the information described above for the first disclosure with an indication of the interval, frequency, or total number of disclosures made during the accounting period, and the date of the last disclosure.

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

The exclusion from the accounting for disclosures does not apply for treatment, payment, and healthcare operations made through an "Electronic Health Record." An "Electronic Health Record" is an electronic record of health-related information on an individual that is created, gathered, managed, or consulted by an authorized health clinician or staff. Effective (i) January 1, 2014 – if the Plan

acquired an Electronic Health Record as of January 1, 2009, or (ii) the later of January 1, 2011 or the date the Plan obtains an Electronic Health Record if the Plan acquired that Electronic Health Record after January 1, 2009:

- ❖ Disclosures of protected health information made by the Plan from an Electronic Health Record for treatment, payment and health care operations during the three (3) years prior to an individual's request are also subject to a request for an accounting.
- ❖ For this purpose, the Plan shall provide an accounting of disclosures of protected health information made by the Plan, and either an accounting of disclosures of protected health information by all Business Associates acting on behalf of the Plan or a list of those Business Associates and contact information, from whom individuals may request an accounting of disclosures they have made.

b. Procedure

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, take the following steps:

- Verify the identity of the individual (or parent or personal representative) following the procedures set forth in **"Verification of Identity of Those Requesting Protected Health Information"** on pages 40 – 42.

- Request that the Individual complete a **"Request for an Accounting of Disclosures of PHI"** form. (See Form "K.")

- The Privacy Officer is responsible for processing requests, determining what disclosures, if any, are not to be included in the accounting, and summarizing multiple disclosures to the same entity or person.

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. The Privacy Officer shall collect any processing fees. All necessary fees must be delivered to the Privacy Officer prior to the provision of additional accountings in the 12 month period.

- 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 University 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.

  * *Except for disclosures made through an Electronic Health Record.*

- If any Business Associate of the Plan has the authority to disclose the individual's PHI, then the University's Privacy Officer or designated University Workforce Member shall contact the appropriate Business Associate to request the disclosure.

- 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.)

- The accounting shall be delivered to the individual requesting the Accounting by mail, e-mail, other mutually agreeable method.

- 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 the Plan receives such a statement, either orally or in writing, contact the Privacy Officer for more guidance.

- An individual may request review by a licensed health care professional, designated by the Plan, if access is denied for one of the following reasons:

  - A licensed health care professional has determined, using professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

  - The PHI makes reference to another person (unless that person is a health care provider) and a licensed health care professional has determined, using professional judgment, that the access requested is reasonably likely to cause substantial harm to the other person; or

  - The request for access is made by the individual's personal representative and a licensed health care professional has determined, using professional judgment, that the provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

- The Plan will provide or deny access based upon the reviewing health care professional's determination.

- If access is denied, in whole or in part, the Plan will:

  - Make accessible any other requested information in the Designated Record Set where the Plan does not believe that there are grounds to deny access.

- Document Accountings in accordance with the **"Documentation Requirements"** beginning on page 49.

- Retain applicable documents for the appropriate six year period.

4. Requests for Confidential Communications

a. Policy

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

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

b. Procedure

Upon receiving a written request – using the University's form (see Form "I") – 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, take the following steps:

- Verify the identity of the individual (or parent or personal representative) following the procedures set forth in **"Verification of Identity of Those Requesting Protected Health Information"** on pages 40 – 42.

- 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.

- Determine whether the request provides for an alternative means of communication (e.g., alternate telephone number) or an alternate location for communication of PHI (e.g., an alternate address).

- Honor requests that include a clear statement that disclosure of the information would endanger the individual.

- Provide a written response (see Form "J"). If a written response is inappropriate, contact the individual in person or by telephone.

- If a request will not be accommodated, 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 by the Privacy Officer.

- Document requests for confidential communications and their dispositions in accordance with the procedure for **"Documentation Requirements"** beginning on page 49.

- Retain all applicable documents for the appropriate six year period.

5. Requests for Restrictions on Uses and Disclosures of PHI

a. Policy

An individual may request restrictions on the use and disclosure of the individual's PHI. It is the University's policy to attempt to honor such requests if, in the sole discretion of the University, the requests are reasonable, except as noted below.

The Plan shall consider, but is not required to agree to any requested restrictions. If the Plan does agree to the restriction, it will comply with the restriction unless the information is needed to provide emergency treatment to the individual. The Plan will comply with an individual's request if (i) the disclosure is to a health plan for purposes of payment or health care operations (not for purposes of treatment) and is not otherwise required by law, and (ii) the protected health information pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full.

All requests for restrictions must be in writing and approved by the Privacy Officer.

b. Procedure

Upon receiving a written request from an individual (or a minor's parent or an individual's personal representative) to restrict access to an individual's PHI, the Workforce Member must take the following steps:

- Verify the identity of the individual (or parent or personal representative) following the procedures set forth in **"Verification of Identity of Those Requesting Protected Health Information"** on pages 40 – 42.

- Request that the individual provide a written request (see Form "G").

- Honor reasonable requests that restrict PHI use or disclosure for purposes of treatment, payment, or health care operations. Take steps to honor requests to restrict information given to persons involved in the individual's care.

- Provide a written response to the individual (see Form "H"). If a written response is inappropriate, contact the individual in person or by telephone.

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

- All requests for restrictions on use or disclosure of PHI that are approved must be tracked by the Privacy Officer or the Privacy Officer's designated staff member.

- Notify all Business Associates that may have access to the individual's PHI of any agreed-to restrictions by the Privacy Officer or the Privacy Officer's designated staff member via facsimile, e-mail, or first class mail.

- Document requests and their dispositions in accordance with the procedure for **"Documentation Requirements"** beginning on page 50.

- Retain applicable documents for the appropriate six year period.

- The Plan will terminate its agreement to honor a restriction only under the following circumstances:

  - The individual agrees to or requests that the restriction terminate;

  - An emergency arises; or

  - The Plan unilaterally terminates its agreement on a prospective basis and notifies the individual in writing of the termination (except the Plan may not unilaterally terminate any agreement to restrict disclosure of PHI for payment or healthcare operations where the individual has paid the healthcare provider in full).

Verification of Identity of Those Requesting Protected Health Information

1. Verifying Identity and Authority of Requesting Party

Workforce Members 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.

a. Request Made by Individual

If the individual's identity and authority is known, no further documentation is necessary.

If the individual's identity and authority is not known, seek verification through one of the following:

- Signature on a written request with a copy of a government issued or University issued photo identification; or

- Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver's license number of the individual who is the subject of the PHI.

And,

- Document disclosures as required by the **"Documentation Requirements"** beginning on page 49.

- Retain all appropriate documents for the applicable six year period.

b. Request Made by Parent Seeking PHI of Minor Child

When a parent requests access to parent's minor child's PHI, take the following steps:

- Verify the person's relationship with the child and confirm the child's age. Verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. Check with Privacy Officer to obtain information about relevant state law.

- Document disclosures as required by the **"Documentation Requirements"** beginning on page 49.

- Retain all appropriate documents for the applicable six year period.

c. Request Made by Authorized Personal Representative

An authorized personal representative is any one of the following:

- A parent, guardian, or other person acting *in loco parentis* for an un-emancipated minor. As a general rule, a parent or guardian is a child's personal representative except under the following circumstances:

  - When the minor is able to lawfully obtain the health care service at issue without the consent of a parent, guardian, or other person acting *in loco parentis*, or
  - When the parent, guardian, or other person acting *in loco parentis* consents to confidentiality between the Plan or health care provider and the minor with regarding to the health care service at issue. (The plan must honor the agreement of confidentiality.)

- An executor, administrator, or other person who has authority to act on behalf of a deceased individual or that individual's estate; or

- A person who has the authority (under applicable state law) to make health care decisions on behalf of an individual who is unable to make health care decisions for himself or herself. (For example, a spouse may have a health care Power of Attorney for an individual who is incapacitated.)

Personal representatives shall not be given access to PHI if Plan representatives have a reasonable belief, based upon professional judgment that the individual at issue has been or may be subjected to domestic violence, abuse or neglect by the person seeking to assert rights as a personal representative.

When a personal representative requests access to an individual's PHI, the following steps should be followed:

- Request and obtain a copy of appropriate documentation such as a valid health care Power of Attorney, or a document permissible under applicable state law. If there are any questions, seek review by the Privacy Officer. Also, if the person claiming to be a personal representative relies upon a document permitted under applicable state law, seek review by the Privacy Officer.

- Appropriate documentation may include one of the following:
  - Guardianship documents;
  - Power of Attorney (for health care decisions);
  - Authorization form naming personal representative; or
  - Other documentation showing authority under applicable state law to act as a personal representative.
- Make a copy of the documentation provided and file it with the individual's Designated Record Set.
- Document disclosures in accordance with the procedure for **"Documentation Requirements"** beginning on page 49.
- Retain all appropriate documents for the applicable six year period.

d. Request Made by Public Official

If a public official requests access to PHI, and if the request is for one of the purposes set forth above in **"Mandatory Disclosures of PHI"** on page 11 or **"Permissible Disclosures of PHI"** on page 13, take the following steps to verify the public 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 Privacy Officer.

- Obtain approval for the disclosure from the Privacy Officer.

- Document disclosures in accordance with the procedure for **"Documentation Requirements"** beginning on page 49.

- Retain all appropriate documents for the applicable six year period.

e. Request Made by Person Involved in Individual's Care

If someone is obviously involved in an individual's care or the payment for that individual's care, PHI may be disclosed to that person, but that person must be a family member, close personal friend, or some other person identified by the individual as being involved in his or her care.

If the individual is present, then the health plan may use or disclose PHI if: (1) the individual provides his or her agreement; (2) the individual has an opportunity to object and does not do so; or (3) from the circumstances, and based on professional judgment, an inference arises that the individual does not object to the disclosure or use.

If the individual is not present for the use or disclosure, or an opportunity to agree or object is not feasible due to an emergency or incapacity, the plan may disclose or use PHI if, in the exercise of professional judgment, it is in the best interest of the individual. For example, if an individual is incapacitated and a spouse calls seeking assistance with payment of claims for the incapacitated individual, PHI may be disclosed to the spouse.

If uncertainty arises regarding whether the disclosure is appropriate, or if it is determined that disclosure is not appropriate, contact the Privacy Officer.

Complying With the "Minimum-Necessary Standard”

a. Policy

The Plan and the University shall take reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose when using or disclosing PHI or seeking PHI from another covered entity. The Plan shall not use, disclose, or request an individual’s entire medical record, even for purposes of payment or health care operations, unless the use, disclosure, or request is justified by the individual circumstances leading to the use, disclosure, or request.

Until the Secretary of Health and Human Services issues guidance, on what constitutes the “minimum necessary” standard, the Plan will limit any use, disclosure or request for protected health information to the limited data set, as set forth in the HIPAA Privacy Rule, or if needed by the Plan, to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The Plan will comply with any future guidance on what constitutes the “minimum necessary” promulgated by the Secretary, which guidance shall override inconsistent policies and procedures established herein. References in this policy to the “minimum necessary” shall be interpreted in accordance with this paragraph.

However, 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 the DOL;
- uses or disclosures required by law; and
- uses or disclosures required to comply with the Privacy Regulations.

For all other recurrent uses and disclosures, the University and the Plan will apply the procedures set forth below.

b. Procedure

(1) Minimum Necessary When Disclosing PHI

For making *disclosures* of PHI:

Routine and Recurring Disclosure	Recipient(s)	Policy & Procedure
Health Market Planning	Insurance Carriers; Brokers; Consultants; Plan Sponsor; Health Plans	Provide summary and de-identified information initially; provide minimum necessary PHI for accurate underwriting

Routine and Recurring Disclosure	Recipient(s)	Policy & Procedure
		(genetic information will not be used for underwriting purposes except for underwriting any applicable long-term care policy)
Budgeting and Renewal	Insurance Carriers; Brokers; Consultants	Provide summary and de-identified information initially; provide minimum necessary PHI for accurate underwriting (genetic information will not be used for underwriting purposes except for underwriting any applicable long-term care policy)
Claim Issue Resolution	Insurance Carriers; Consultants; Providers	First, direct individual to Carrier. Second, obtain written authorization for Human Resources Department Workforce Member to assist.
Compliance Issue Resolution	Outside legal counsel; Brokers; Consultants	Provide minimum details of PHI necessary to secure legal counsel.
Claims Audit	Brokers/Consultants; Providers; Claims Review Specialists	Provide summary and de-identified information and PHI only if required
Billing Issue Resolution	Insurance Carriers; Consultants; Providers	Provide summary and de-identified information and PHI only if required
COBRA Rate or Funding Level Determination	Insurance Carriers; Brokers; Consultants	Provide summary and de-identified information and PHI only if required
Network Discount Evaluation	Insurance Carriers; Brokers; Consultants	Provide summary and de-identified information and PHI only if required
Disruption Analysis	Insurance Carriers; Brokers; Consultants	Provide summary and de-identified information and PHI only if required
Strategic Planning	Insurance Carriers; Brokers; Consultants	Provide summary and de-identified information and PHI only if required
Modifying, Amending, or Terminating the Group Health Plan	Plan Sponsor	Provide summary information

Routine and Recurring Disclosure	Recipient(s)	Policy & Procedure
Enrollment or Disenrollment Information	Plan Sponsor	Provide enrollment or disenrollment status information only
Plan Administration	Plan Sponsor	To the extent necessary for plan administration so long as plan sponsor has amended its plan documents in accordance with the HIPAA Privacy Regulations

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

(2) Minimum Necessary When Requesting PHI

For making *requests* for disclosure of PHI:

Routine and Recurring Requests	Disclosing Entity	Policy & Procedure
Health Market Planning	Carriers; brokers; consultants	Request summary and de-identified information and PHI only if needed
Budgeting Underwriting and Experience Evaluation	Carriers; brokers; consultants	Request summary and de-identified information and PHI only if needed (genetic information will not be used for underwriting purposes except for underwriting any applicable long-term care policy)
Claim Issue Resolution	Carriers; Consultants; Providers	Request summary and de-identified information and PHI only if needed
Compliance Issue Resolution	Outside legal counsel; individual; carrier; brokers; consultants	Request summary and de-identified information and PHI only if needed
Claims Audit	Insurance carrier	Request summary and de-identified information and PHI only if needed
Billing Issue Resolution	Insurance Carriers; Consultants; Providers	Request summary and de-identified information and PHI only if needed

Routine and Recurring Requests	Disclosing Entity	Policy & Procedure
COBRA rate or funding level determination	Insurance Carriers	Request summary and de-identified information and PHI only if needed
Network discount evaluation	Insurance Carriers	Request summary and de-identified information and PHI only if needed
Disruption Analysis	Insurance Carriers	Request summary and de-identified information and PHI only if needed
Strategic Planning	Insurance Carriers; Consultants/Brokers	Request summary and de-identified information and PHI only if needed

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

(3) Minimum Necessary When Receiving or Disclosing PHI for employment-related purposes

For receiving PHI for employment-related purposes:

Routine and Recurring Disclosures and Requests	Recipient(s)/ Disclosing Entity	Policy & Procedure
Benefits inquiries and assisting with claims issues	Insurance carrier; Third Party Administrators; Brokers; Consultants	Obtain written authorization for disclosure of PHI.
Obtaining a determination as to whether employee can perform essential functions of job and conclusions related to a fitness-for-duty exam	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; PHI obtained for performance of essential functions of a job or for a fitness-for-duty examination shall be filed in the applicable employee's medical file.
Obtaining results from drug-testing for employment-related reasons	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; drug testing results shall be filed in the applicable employee's medical file.

Routine and Recurring Disclosures and Requests	Recipient(s)/ Disclosing Entity	Policy & Procedure
Responding to a request for an accommodation under the Americans with Disabilities Act.	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; responses shall be filed in the applicable employee's medical file.
Responding to a request for a leave of absence under the Family and Medical Leave Act	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; physician's certification shall be filed in the applicable employee's medical file.

Disclosures of De-Identified Information

a. Policy

The Plan may freely use and disclose 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 (1) professional statistical analysis conducted in accordance with the Privacy Regulations; or (2) removing 18 specific identifiers. These identifiers are as follows:

- Names;
- Geographic subdivisions smaller than State, including street address, city, county, precinct, ZIP code, and equivalent geocodes (special rules apply);
- All elements of dates (except year) relating directly to an individual (special rules apply);
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical Record Numbers;
- Health Plan beneficiary numbers;
- Account Numbers;
- Certificate/license numbers;
- Vehicle identification and serial numbers (including license plate numbers);
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (special rules apply).

b. Procedure

To use or disclose De-identified Inforamtion, follow the following steps:

- Obtain approval from Privacy Officer for the disclosure. The Privacy Officer will verify that the information is de-identified.

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

Documentation Requirements

a. Policy

The Plan and the University shall retain required documents – either in written or electronic form – for six years from either the date the documents were created or the date the documents were last in effect, whichever is later.

b. Procedure

Documentation. The Plan 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:

- "Privacy Notices" issued to participants (copy of Notice shall be maintained in a file by Privacy Officer).

- Records of non-treatment, payment, health care operations disclosures or as set forth in the exceptions listed below (disclosure documents maintained by firewall Workforce Members and monitored by Privacy Officer):

  - 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.
  - See Form “P” for the “Protected Health Information Disclosure” form.

- Completed Protected Health Information Disclosure forms shall be maintained in an individual’s Designated Record Set for the applicable six year period.

- Documentation of disclosures is not required if PHI is disclosed for any of the following:

  - for treatment, payment, or health plan operations;
  - to the individual (or his or her personal representative) about himself or herself;
  - for a facility directory, to next-of-kin, or to those involved in an individual’s care;
  - for national security or intelligence purposes;
  - to correctional institutions or law enforcement officials;
  - based on an individual authorization;

- as part of a limited date set; or
- incidental to another permissible use or disclosure.

- Signed individual authorizations (maintained in Designated Record Set by Privacy Officer).

- Business Associate Agreements with Business Associates (maintained by Privacy Officer).

- Plan documents (maintained by Plan Administrator).

- University Policies on use and disclosure of PHI (maintained by Privacy Officer).

- Documentation concerning the following individual rights (maintained by the Privacy Officer):

  - The designated record set subject to inspection and copying by an individual;
  - The name and title for the person or office receiving and responding to requests to amend or copy PHI;
  - Any written requests for amendment and responses to requests for amendment (including the written denial, statements of disagreement, and the Plan's rebuttal, if any); and
  - Any agreed-upon restrictions on the use and disclosure of an individual's PHI.

- Designation by Business Associates and Insurance Carriers of who can receive and/or discuss PHI of individuals participating in the Plan (maintained by Privacy Officer).

- Individual complaints and the outcome of the complaints (documentation to be maintained by the Privacy Officer).

- Records (maintained by the Privacy Officer) of any sanctions imposed on any employees, agents, subcontractors, or Business Associates for violations of these policies and procedures or the Privacy Regulations.

- Information on whether the Plan is part of an organized health care arrangement (maintained by the Privacy Officer).

- Workforce Member HIPAA Privacy Regulations training materials (maintained by the Privacy Officer).

- Certification of the Plan Sponsor regarding plan amendments and firewalls (maintained by the Privacy Officer).

- Documentation of any other action, activity, or designation (such as the designation of the Privacy Officer) required to be documented by the Privacy Regulations.

Documentation may be maintained or created in written or electronic form.

Security Policies and Procedures

1. Physical and Technical Security

a. Policy

The University and the Plan will maintain the physical and technical security of the Plan's PHI.

The University and the Plan shall take reasonable measures to ensure that only designated Workforce Members shall have access to PHI concerning individuals in the Plan.

The Privacy Officer and appropriate supervisors or managers shall determine the necessary level of access for each firewall Workforce Member. Each firewall Workforce Member shall be given physical access to PHI in accordance with his or her necessary level of access. Access should be limited sufficiently to afford Plan members as much privacy and security as possible without limiting access so as to interfere with the efficiency of Plan administration.

b. Procedures

(1) PHI Storage and Access

Physical Security: To maintain physical security of PHI, the Plan and the University will follow these safeguards in a reasonable manner:

- Maintenance of Primary Physical Security –
  - The University's human resources department offices will maintain a secure reception area with a receptionist on duty and/or a locked door accessible only to Workforce Members via an electronic card or code mechanism; and
  - Visitors will be escorted to their contact person and not left unattended.
- Maintenance of Secondary Physical Security –
  - All files containing PHI, including diskettes and CDs, are to be kept in a separate file area of the human resources or an enclosed room or locked desk where access is limited to those Loyola University New Orleans Workforce Members who have access per the terms of the Loyola University New Orleans Privacy Policy.
  - Workforce Members with access to PHI shall not leave files, electronic storage media, or documents containing PHI on desktops, countertops, or

work tables unattended. Files or documents containing PHI may be kept at Workforce Member desks provided that they are not left unattended on the Workforce Member's desktop and are kept in locked drawers when not in use.

- Each firewall Workforce Members is expected to use reasonable efforts to protect PHI during and after work hours in areas under the Workforce Member's control such as employee offices, workstations, desks, and filing areas.

- If a firewall Workforce Member leaves his or her desk for a short period of time, the Workforce Member should conceal materials containing PHI to prevent accidental viewing.

- If a firewall Workforce Member leaves his or her desk for an extended period of time or at the end of the workday, the Workforce Member should make certain that all materials containing PHI are placed in a secure location such as a locked desk drawer or filing cabinet.

- Documents containing PHI should not be left unattended on computers, copiers, fax machines, or printers.

- PHI should be protected in any form – electronic copy, hard copy, computer screen, or any other form of duplication for an original.

- Documents or electronic media containing PHI should not be deposited in trash cans, unsecured recycling bins, or other unsecured containers. PHI shall be destroyed in accordance with the University's document destruction policy.

- Where reasonable and appropriate, PHI will be secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals. The amount of unsecured PHI maintained by the Plan should be limited.

    - ❖ Acceptable means to render PHI unusable, unreadable, or indecipherable are encryption and destruction.
    - ❖ The method to render PHI unusable, unreadable, or indecipherable shall be reviewed on an annual basis by the Security Officer to determine if the methodology or technology meets the current standards set by HHS.

- Files containing PHI shall be clearly labeled as "private and confidential."

- Verbal Security –

  - Workforce Members shall take reasonable care in verbally discussing PHI to ensure that PHI is not discussed with any employee, individual, or third party who does not have access under the terms of the University's Privacy Policy.

  - When using the telephone to discuss PHI, Workforce Members shall take reasonable care to make sure that the party to whom they are speaking has access to PHI and is either the individual who is the subject matter of the PHI, is the individual's personal representative, or is an individual, designated by a Business Associate, and insurance carrier, or a health care provider, to be contacted about PHI concerning individuals in the Plan.

  - PHI should not be discussed in public areas such as cubicles, elevators and lunch rooms or at social gatherings.

- Security Maintenance –

  - The Privacy Officer will monitor physical and verbal security and access to files containing PHI.

  - Supervisory and management personnel will review the location and placement of all computer displays, printers, copiers, and fax machines on a periodic basis to determine whether any changes should be made in order to comply with the University's Privacy Policies and Procedures and make any necessary changes.

  - If necessary, a risk and cost analysis shall be undertaken to determine whether physical changes are needed to improve security. Any such risk analysis shall be documented. All documentation should be forwarded to the Privacy Officer and shall be retained for six (6) years.

  - Workforce Members handling PHI shall report any violations of the University's Privacy Policy to the Privacy Officer as soon as possible, but no later than three business days after the incident occurs.

- Access to PHI –

  - Each firewall Workforce Member shall be advised of his or her level of access to PHI.

  - The Privacy Officer and appropriate supervisors or managers will make certain that physical access to PHI shall be limited to firewall Workforce Members. Necessary steps shall include making sure that only firewall Workforce Members have keys to filing cabinets containing documents with PHI and that only firewall Workforce Members have access to drawers or

work areas with materials containing PHI and workstations or electronic media containing PHI.

- Upon termination of a firewall workforce member's employment or other arrangement, or a change in assignments requiring a decreased level of access to PHI, the firewall Workforce Member's supervisor shall notify the IT department and the Privacy Officer (Form "T"). The notice shall include the date that access is terminated or modified, the Workforce Member's name, and a description of the Workforce Member's access privileges. The Privacy Officer, or his or her designated representative, shall ensure that applicable access privileges are revoked or changed and that appropriate third parties are notified of the termination or decreased level of access to PHI. Relevant keys, cards, passwords, or electronic access should be returned or changed, as applicable.

- Destruction of PHI –

  - Discarded PHI shall be left completely inaccessible.

  - PHI in any form (hard copy, diskette, CD, etc.) shall not be discarded in ordinary trash.

  - Diskettes, CDs or other electronic media containing PHI must be erased or destroyed. Electronic media must be cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the Protected Health Information cannot be retrieved.

  - Paper, film or other hard copy media is to be shredded or destroyed such that the Protected Health Information cannot be read or otherwise cannot be reconstructed. Redaction is not an appropriate means of data destruction.

  - Photocopiers with hard drives or other storage of information that are to be discarded or leased machines that are to be returned must have the hard drives erased using NIST standards before being disposed or returned.

Electronic Security: The Plan shall implement such procedures and policies and necessary to comply with the HIPAA Security regulations.

(2) PHI Transmission

For transmission of PHI, follow these procedures:

- Incoming Mail –

  - Incoming mail containing PHI should be delivered unopened in its original sealed envelope to the person to whom it is addressed.

- Workforce Members with access to PHI under the Privacy Policy should request that their business contacts – such a consultants and insurance carriers – clearly indicate the name of the specific person at the University and be labeled "confidential" on the envelope.

- If a Workforce Member receives PHI and the Workforce Member is not permitted access to PHI under this Privacy Policy, the Workforce Member should redirect the incoming mail as soon as possible to an appropriate person with access to PHI.

- Outgoing Mail –

  - Outgoing mail containing PHI should be clearly addressed to a specific person and be labeled "confidential."

  - If the outgoing mail contains PHI and is to be sent to an organization, it should be specifically addressed to a person at the organization who has access to PHI as per the organization's policies and procedures.

- Inbound E-mail –

  - Workforce Members with access to PHI should exercise reasonable care to keep incoming e-mail messages secure and limit access by other University Workforce Members.

  - Substantive e-mails containing PHI may be printed out at a secure printer for hard copy storage in secured files maintained by the human resources department.

  - Workforce Members receiving PHI should request that persons sending e-mails limit the number of people that are copied on e-mails in order to limit the opportunity for inadvertent disclosure of PHI. The Privacy Officer will provide third-party administrators, carriers, and other service providers should a list of individuals authorized to receive PHI on behalf of the Plan. The Privacy Officer shall request that PHI sent via email to the Plan be sent to an individual identified on the applicable list.

  - If a Workforce Member, who does not have access to PHI under this Policy, receives PHI, the Workforce Member should forward the e-mail to someone who does have access under this Policy as soon as possible. The Workforce Member who improperly received the e-mail should delete the e-mail from his or her inbox, sent mail, and trash or deleted email folders after forwarding the e-mail to the appropriate person.

- Outbound E-mail –

- E-mail sent externally from University locations may be transmitted to outside contacts provided that any file attachments containing PHI are password protected and individually identifiable information is not contained in the subject line. The password may be communicated via phone or fax, or in a separate e-mail significantly (one hour or more) prior to or after the e-mail containing the file with the PHI.

- E-mail containing PHI sent internally in the University's offices may be transmitted provided that any individually identifiable information is not contained in the subject line.

- Outbound e-mail should also contain the following disclaimer:

"This e-mail and any files transmitted with it are intended only for the person or entity to which it is addressed and may contain confidential material and/or material protected by law. Any retransmission or use of this information may be a violation of that law. If you received this in error, please contact the sender and delete the material from any computer."

- Incoming Faxes –

  - Facsimile (fax) machine transmissions containing PHI sent to the human resources department shall be made using a fax machine dedicated to the Human Resources Department in a secure location.

- Outgoing Faxes –

  - When sending a fax, use a cover page containing the name of the recipient, the fax number, and the number of pages. Include a label stating that the fax is "confidential." Do not include any PHI on the cover page.

  - Faxes containing PHI sent from the human resources department to Workforce Members shall be sent to a fax machine attended by the specific recipient. If necessary, the recipient should be telephoned prior to sending the fax.

  - If a Workforce Member receives PHI and the employee does not have access to the PHI, the Workforce Member should redirect the fax as soon as possible.

  - Faxes containing PHI sent to insurance carriers, consultants, brokers, other Business Associates, or entities for purposes of treatment, payment, or health care operations shall be sent to a specific person at the receiving organization and only to persons at that organization designated as having access to the Plan's PHI.

- Outgoing faxes containing PHI should include the following disclaimer on a cover sheet:

"The documents accompanying this facsimile contain confidential information and/or material protected by law. The information is intended only for the use of the individual or entity named above. If you are not the intended recipient, any retransmission or use of this information may be a violation of that law. If you received this facsimile in error, please immediately notify us by telephone to arrange for return of the original documents to us."

- Cover sheets should be verified immediately before and after transmission of PHI to confirm that the information was sent to the correct fax number and was addressed to the correct recipient. If the PHI is not sent to the correct fax number, the sender should immediately send another fax to the number contacted in error with a reminder that the information sent is confidential and a request that the that the recipient contact the sender to arrange for proper destruction of the information. Any such error must be immediately reported to the Privacy Officer and recorded as an accidental disclosure of PHI.

    - The Privacy Officer will maintain all documentation regarding such an accidental disclosure for the applicable six (6) year period.
    - If necessary, the Privacy Officer shall contact legal counsel.

- Diskette/CD and other portable electronic media such as DVDs, flash drives, thumb drives, hard drives, laptops, etc. –

    - Follow the same policy for receiving and sending mail as described above.

- Internet –

    - Do not download PHI from, or upload PHI to, any web site or system via the Internet other than to an insurance carrier or business associate unless the site is a secure site that can be accessed via a secure link (SSL). This means that the site can be accessed using a secure, encrypted connection as required by the Privacy Regulations. When uncertain if a site is secure, check with IT.

    - Workforce Members may use the secure system of an insurance carrier, a service provider, or a Business Associate via their web site to communicate PHI. In other words, the PHI must reside on a secure system belonging to the service provider, insurance carrier, or Business Associate.

    - Take reasonable care to protect PHI from access by individuals who are not authorized to access it.

(3) PHI Storage Related to Terminated Workforce Members

- Physical Storage – PHI for terminated Workforce Members shall be protected in the same manner that it was protected prior to the Workforce Member's termination of employment or other arrangement.

  - The former Workforce Member's file PHI shall be retained for a period of six years following the date it was created or the date it was last in effect, whichever is later.

(4) Electronic PHI

- Securing Electronic PHI

  - When deemed appropriate by the Privacy Officer and the Security Officer, electronic PHI shall be encrypted by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Decryption tools must be stored on a device or at a location separate from the data they are used to encrypt or decrypt.

    - Data at rest: data that resides in databases, file systems, flash drives, memory and any other structures storage system, must be encrypted consistent with National Institute of Standards and Technology, or "NIST," Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.

    - Data in motion: data that is moving through a network, including wireless transmission, whether by email or structured electronic interchange, must be encrypted consistent with NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standards 140-2 validated.

Violation Policy and Procedures

1. Complaints

Donna Rochon, the Privacy Officer for the Loyola University New Orleans Employee Benefit Plan, Human Resources Department, Loyola University New Orleans, 6363 St. Charles Avenue, Campus Box 16, New Orleans, LA 70118, 504.864.7272 (phone), 504.864.7100 (fax), will be the Plan's contact person for receiving complaints.

Individuals will use the following process to lodge complaints about the University's privacy procedures. Written complaints shall be received by the Privacy Officer, who shall promptly notify the Privacy Officer of any such complaints. Individuals making a written complaint should use Form "M," but are not required to use Form "M." Oral complaints may be made directly to the Privacy Officer. The Privacy Officer shall conduct an investigation into all complaints and shall make findings and recommend any necessary actions. The Privacy Officer's findings and recommendations should be in writing. A Complaint Review form (Form "N") shall be completed in connection with each complaint received. Complaints and documents reflecting the disposition of the complaints shall be retained for six years.

A copy of the complaint procedure shall be provided to any individual upon request. Individuals shall be notified of where to send complaints in the Privacy Notice and applicable forms.

There will be no retaliation, reprisal, or intimidation against anyone for reporting a violation of this Policy or the Privacy Regulations, or for cooperating with an investigation of a complaint under this Policy. The University's policy is to investigate each complaint promptly and to keep complaints and the result of any investigation confidential to the fullest extent practicable.

2. Notification of Privacy Officer

Any Workforce Member who believes that a violation of this Policy has occurred is required to contact the Privacy Officer immediately. In a confidential manner, the Privacy Officer will investigate the facts and circumstances of the alleged violations and determine an appropriate course of action.

3. Sanctions for Violations of Privacy Policy

If the Privacy Officer determines that a violation of the University's Privacy Policy has occurred, all involved parties (such as the individual whose PHI was improperly disclosed or used, the Business Associate or insurance carrier, and any other University Workforce Member) will be notified in a timely manner. The Privacy Officer will conduct an investigation into the alleged violation in a timely manner. If a violation has occurred, resolution of such violation will seek to restore the level of privacy and security that is required under this Policy. Any deficiency in the University's Privacy

Policy or related procedures that contributed to the violation will be corrected. If monetary damages are found to be due, then this issue will be settled by the Privacy Officer or the Employer's legal counsel under the laws of the state in which the individual whose PHI was improperly used or disclosed resides.

The Workforce Member(s) responsible for the violation will be dealt with according to standard University disciplinary practices. The disciplinary action will depend upon the severity and/or frequency of the violation and whether the violation was blatant. Disciplinary action may range from, but is not limited to, a verbal warning, written warning, probation, up to and including termination of employment.

In investigating complaints under this policy, the University may impose discipline for inappropriate conduct without regard to whether the conduct constitutes a violation of the law and even if that conduct does not rise to the level of violation of this policy. Appropriate parties will be advised of the outcome of an investigation, although not necessarily all details of the actions the University has taken to maintain the provisions of this Policy.

Sanctions for using or disclosing PHI in violation of this Policy will be imposed, up to and including termination. Individuals who inadvertently use or disclose PHI will be subject to a verbal or written warning. Individuals who blatantly and purposefully use or disclose PHI without regard for this Policy will be subject to having their employment terminated. The Privacy Officer shall document all sanctions and retain applicable records for six years.

4. Mitigation of Inadvertent Disclosures of Protected Health Information

The University 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 the policies and procedures set forth in this Policy. As a result, if a Workforce Member becomes aware of a use or disclosure of Protected Health Information, either by a Plan Workforce Member or a Business Associate or another outside entity, that is not in compliance with this Policy, the Workforce Member should immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the individual can be taken.

The Privacy Officer shall act to stop the violation as soon as possible. Necessary steps may include, but not be limited to, suspending access privileges to PHI.

5. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy Rights

No Workforce Member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Regulations, in good faith. However, if the Workforce Member reporting the violation is also the source of the violation, appropriate sanctions may be asserted against that Workforce Member.

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

6. Violation Tracking

The Privacy Officer will track all reported incidents of potential violation under this Policy whether or not a reported incident is ultimately found to be an actual violation. Tracking includes maintaining the relevant facts of a reported incident and the final determination or resolution.

Breach of Information Policy and Procedures

1. Breach of Information

a. Policy.

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.

In order to constitute a breach, which triggers the notification requirement, the following conditions must be met:

- *The information breached is PHI*. The breach notification requirement does not apply to information that is not PHI – such as de-identified information.

- *There has been an unauthorized acquisition, access, use or disclosure*. Unauthorized means acquisition, access, use or disclosure of PHI that compromises the privacy or security of that information. If there is no HIPAA privacy violation, there is no breach. Uses or disclosures involving more than the minimum necessary amount may qualify as a breach.

- *Compromises the security or privacy of the protected health information*. An impermissible use or disclosure of PHI is presumed to be a breach unless there is a demonstration of a low probability that the PHI has been compromised. Notification to impacted individuals is necessary in all situations except when there is a demonstration of a low probability of harm or that an exception to the breach notification rule applies. In order to assess the probability that the PHI has been compromised, the Privacy Officer will consider the following: (1) the nature and the extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the PHI was disclosed; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.

The following shall not be considered breaches:

- Unintentional acquisition, access or use of protected health information by a Workforce Member or individual acting under the authority of a covered entity or Business Associate, if the acquisition, access, or use was made in good faith, within the course and scope of employment or other professional relationship, and does not result in further use or disclosure. For example, if a billing employee opens an e-mail with PHI mistakenly sent by a nurse, this would not be a breach if the billing employee realizes he is not the intended recipient, notifies the nurse of the mistake and deletes the e-mail.

- Inadvertent disclosure of PHI from a person who is authorized to access PHI at a facility operated by a covered entity or a Business Associate to another similarly situated person authorized to access PHI at the same facility if the information is not further acquired, accessed, used or disclosed without authorization. Inadvertent disclosures of PHI from a person who is authorized to access PHI at a covered entity or Business Associate to another person authorized to access PHI at the same covered entity or Business Associate are also exceptions.

- The unauthorized person to whom PHI has been disclosed would not reasonably have been able to retain the information. HHS gave two examples. In the first example, a health plan sends EOBs to the wrong person. The envelopes are returned by the post office unopened and marked undeliverable. In this case no breach occurred. If, however, any of the envelopes are not returned, this should be treated as a potential breach. In the second example, a nurse hands a patient someone else's discharge papers, but realizes her mistake and recovers the papers quickly. If the nurse can reasonably conclude that the patient could not have read the information, this would not be a breach.

All workforce members are responsible for immediately reporting breaches or potential breaches of unsecured PHI. Workforce members may report breaches or potential breaches to their manager or the Privacy Officer. If a report is made to a manager, the manager shall immediately report the potential breach to the Privacy Officer.

b. Procedure.

The Privacy Officer shall be responsible for investigating all reported incidents of possible breaches in the security or privacy of PHI held by the Plan. After investigation and determination that an actual breach occurred, the Privacy Officer shall take necessary steps to investigate to determine if a breach has occurred, mitigate harm to the extent feasible, provide required notifications, and take steps to reduce the likelihood that that similar breaches occur in the future.

The Privacy Officer shall maintain a Privacy Breach Incident File. In the event of a PHI privacy or security violation, the following steps shall be taken:

(1) Report of Possible Breach.

Any Workforce Member or other individual (such as a Business Associate) who becomes aware of a possible breach of the privacy or security of PHI maintained by the Plan shall report the alleged breach to the Privacy Officer.

The Privacy Officer shall then take the following steps:

- Ask the Workforce Member or other individual reporting the breach to provide the details of the alleged breach in writing (Form "V").

- Review the written summary and determine if further investigation is necessary.

- Conduct an investigation. Determine the following:

  - Whether a breach has occurred.

  - If a breach occurred, what level of breach occurred:

    - Very serious – a large amount of data, or very sensitive data was improperly disclosed.
    - Serious – a large amount of data has potentially been improperly disclosed, but the likelihood of access is slight.
    - Important – protected participant data has been inappropriately released to a business partner.
    - Minor – protected participant data has been handled carelessly, but no exposure occurred.

  - If a breach occurred, what level of culpability exists:

    - Very serious – Workforce Member or other individual engaged in malicious misconduct.
    - Serious – Workforce Member willfully ignored established policies and procedures.
    - Important – Workforce Member inadvertently failed to follow established policies and procedures.
    - Minor – Workforce Member made an error in judgment based on a misunderstanding of the policies or procedures.
    -

- If a breach of privacy or security may have occurred, create a Privacy Potential Breach Incident File. The File shall contain the following:

  - The Report of Privacy Incident Review (Form “W”).
  - The original written summary of the alleged breach.
  - The intended course of action to investigate the alleged breach.
  - Documentation of the investigation, including any documentation related to any interviews.
  - All correspondence related to the alleged breach, including correspondence with legal counsel, if any, which shall be marked as “privileged and confidential.”
  - Documentation of the decision as to whether a breach occurred and any steps taken to resolve the issue.

- Document any data or physical materials that may have been compromised, lost, destroyed, or stolen.

- For serious and very serious situations, inclusion of outside legal counsel.
- For serious and very serious situations, inclusion of professional, state and/or HIPAA oversight agencies such as the Office of Civil Rights.

- Develop an action plan, including the following;

  - Steps to be taken to determine the actual cause of the breach.

  - A determination of whether policies and procedures need to be changed to prevent future breaches, and if so, which policies and procedures.

  - Steps to contact affected individuals whose PHI has been or is reasonably believed to have been compromised by the breach.

    - Provide notice (Form "X"), which must be written in plain language and contain the following:

      - A brief description of what happened, including the date of the breach, if known, and the date of the discovery of the breach;
      - A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
      - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
      - A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
      - Contact procedures for individuals to ask questions or learn additional information.
      - A toll-free number, an e-mail address, web site, or postal address.

    - Provide notice as soon as possible, but no later than 60 days after the date of discovery.

    - Notice must be provided by first class mail, unless only insufficient or out-of-date contact information exists. If only insufficient or out-of-date contact information exists, the following steps must be used:

      - If there are fewer than 10 individuals who cannot be contacted by first class mail, then notice may be made

using an alternative notice such as by e-mail, by telephone, or by other appropriate method.

- If there are 10 or more individuals who cannot be located by first class mail, then an alternative notice must be posted on Loyola University New Orleans' website for at least ninety (90) days in a conspicuous location, or it must be posted in a major print or broadcast media where the affected individuals most likely live. The notice must also include a toll-free number to call for more information. The toll-free number shall be active for at least ninety days.

- If a breach affects the protected health information of 500 or more individuals, the Privacy Officer shall notify the Department of Health and Human Services ("HHS") as required by HIPAA (Form "Y") within 60 days. Sixty days is an outer limit but may be a reasonable time for providing the notification of Breach depending upon the facts and circumstances. If a breach affects the protected health information of fewer than 500 individuals, the Privacy Officer shall log the breaches and report all breaches on an annual basis and no later than 60 days after the end of the calendar year in which the breaches were discovered. Instructions along with a list of the data elements required by HHS and the website address are contained in Form Y.

- If a breach of Unsecured Protected Health Information involves more than 500 residents of a single State or jurisdiction, notification shall be provided to prominent media outlets serving the State or jurisdiction without unreasonable delay and in no case later than 60 calendar days after Discovery of the Breach. (See Form Z for a Sample Press Release.) Sixty days is an outer limit but may not be a reasonable time for providing the notification of Breach depending upon the facts and circumstances.

- If a law enforcement agency requests that the notice to individuals and the media be delayed on the grounds that notice may impede a criminal investigation or national security, the notice must be delayed, but for no more than 30 days. See Request Made by Public Official beginning on page 42 for procedures on identification of law enforcement personnel prior to disclosure PHI.

➢ Appropriate consequences for any responsible Workforce Member(s).

- Changes, if any, necessary to policies and procedures to prevent future similar breach.

- Include Action Plan in the Privacy Incident File.

(2) Concluding Investigation.

Upon conclusion of investigation into a potential breach, the Privacy Officer shall take the following steps:

- Document the outcome of the investigation in the Privacy Incident File.
- Administer and document any necessary sanctions and disciplinary actions.
- Make changes, if necessary, to policies and procedures.

APPENDIX A

Arthur J. Gallagher & Co.
COBRA Professionals, Inc.
Worxtime
UnitedHealthcare

APPENDIX B
FORMS

Form A – Authorization

Form B – Revocation of Authorization

Form C – Individual Request to Inspect and Copy Protected Health Information

Form D – Response to Individual Request to Inspect and Copy Protected Health Information

Form E – Individual Request to Correct or Amend a Record

Form F – Response to Individual Request to Correct or Amend

Form G – Individual Request for Restrictions on Use or Disclosure of Protected Health Information

Form H – Response to Individual Request for Restrictions on Use or Disclosure of Protected Health Information

Form I – Individual Request for Confidential Communication of Protected Health Information

Form J – Response to Individual Request for Confidential Communication of Protected Health Information

Form K – Individual Request for an Accounting of Disclosures of Protected Health Information

Form L – Statement of Disagreement with Response to Request to Amend or Correct a Record

Form M – Complaint Form

Form N – Complaint Review Form

Form O – Employee Confidentiality Agreement

Form P – Protected Health Information Disclosure

Form Q – Personal Representative Designation

Form R – Acknowledgement of Continued Obligation to Maintain Confidentiality of PHI

Form S – Security Access Worksheet

Form T – Notice of Termination of PHI Access

Form U – [Reserved]

Form V – Report of Security Incident Review Form

Form W – Report of Privacy Incident Review Form

Form X – Sample Breach Notice to Individual

Form Y – Notice to Secretary of HHS of Breach of Unsecured Protected Health Information

Form Z – HIPAA Security Breach Notification Sample Press Release