

# **The University of Scranton**

## **HIPAA Privacy Policy**

### **Introduction**

The University of Scranton sponsors and self-funds a group health plan (the Plan). Members of the University's workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the University, for administrative functions of the Plan.

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

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

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

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

### **Plan's Responsibilities as Covered Entity**

#### **I. Privacy Official and Contact Person**

Joseph P. Cortese will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the University's use and disclosure procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

## **II. Workforce Training**

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

## **III. Technical and Physical Safeguards and Firewall**

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

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

## **IV. Privacy Notice**

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

- the uses and disclosures of PHI that may be made by the Plan;
- the individual's rights; and
- the Plan's legal duties with respect to the PHI.

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

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

- no later than April 14, 2004
- on an ongoing basis, at the time of an individual's enrollment in the Plan or, in the case of providers, at the time of treatment and consent; and
- within 60 days after a material change to the notice.

The Plan will also provide notice of availability of the privacy notice at least once every three years.

## **V. Complaints**

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

## **VI. Sanctions for Violations of Privacy Policy**

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with The University of Scranton corrective action policy, up to and including termination. The Corrective Action Policy is defined in The Human Resources Handbook for Staff and Administrators.

## **VII. Mitigation of Inadvertent Disclosures of Protected Health Information**

The University shall mitigate, to the extent possible, any harmful effects that become known to it because 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 an employee becomes aware of a disclosure of protected health information, either by an employee of the Plan or an outside consultant/contractor that is not in compliance with this Policy, immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the participant can be taken.

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

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

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

## **IX. Plan Document**

The Plan document shall include provisions to describe the permitted and required uses and disclosures of PHI by the University for plan administrative purposes. Specifically, the Plan document shall 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 agents or subcontractors 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;
- report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures;

- make the University's internal practices and records relating to the use and disclosure of PHI received from the Plan available to DHHS upon request; and
- 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. The Plan document must also require the University to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the University agrees to those restrictions; and (2) provide adequate firewalls.

## **X. Documentation**

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

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

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

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

## **Policies on Use and Disclosure of PHI**

### **I. Use and Disclosure Defined**

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

- *Use*. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the benefits area of the University, or by a Business Associate (defined below) of the Plan.
- *Disclosure*. For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the benefits area of the University.

### **II. Workforce Must Comply With University's Policy and Procedures**

All members of the University's workforce who have access to PHI (described at the beginning

of this Policy and referred to herein as "employees") must comply with this Policy and with the University's use and disclosure procedures, which are set forth in a separate document.

### **III. Access to PHI Is Limited to Certain Employees**

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

- Benefits Manager and Benefits Human Resource Assistant who perform functions directly on behalf of the group health plan; and
- Benefits Manager, Benefits Human Resource Assistant, Human Resource Assistant, Payroll Manager, Student Payroll Coordinator and Human Resource Director, who have access to PHI on behalf of the University for its' use in "plan administrative functions".

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

### **IV. Permitted Uses and Disclosures: Payment and Health Care Operations**

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

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

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

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

- conducting quality assessment and improvement activities;

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

#### **V. No Disclosure of PHI for Non-Health Plan Purposes**

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

#### **VI. Mandatory Disclosures of PHI: to Individual and DHHS**

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

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

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

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The University's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Plan's Privacy Official. Permitted 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 cadaver organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;

- for specialized government functions; and
- that relate to workers' compensation programs.

### **VIII. Disclosures of PHI Pursuant to an Authorization**

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

### **IX. Complying With the "Minimum-Necessary" Standard**

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

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

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

*Minimum Necessary When Disclosing PHI.* For making *disclosures* of PHI to any Business Associate or providers for claims payment/adjudication, plan design and pricing or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

All other disclosures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

*Minimum Necessary When Requesting PHI.* For making *requests* for disclosure of PHI from Business Associates, providers or Plan Participants for purposes of claims payment/adjudication, plan design and pricing or internal/external auditing purposes, only the minimum necessary amount of information will be requested.

All other requests must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

### **X. Disclosures of PHI to Business Associates**

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the

information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place.

*Business Associate* is an entity that:

- performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

## **XI. Disclosures of De-Identified Information**

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 professional statistical analysis, or by removing 18 specific identifiers.

## **Policies on Individual Rights**

### **I. Access to Protected Health Information and Requests for Amendment**

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

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

### **II. Accounting**

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

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

- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure or pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for other national security or law enforcement purposes.

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

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

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

### **III. Requests for Alternative Communication Means or Locations**

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

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

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

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the University's policy to attempt to honor such requests if, in the sole discretion of the University, the requests are reasonable. The Benefits Department is charged with responsibility for processing requests for restrictions.