UNM HUMAN RESOURCES

HIPAA COMPLIANCE POLICY FOR CERTAIN HEALTH PLANS OFFERED BY THE UNIVERSITY

Effective: July 1, 2009
Subject to Change Without Notice

Authorized by Regents Policy 2.13.4 "University HIPAA Compliance Policy"

1. General

The University sponsors and administers one or more group health benefit plans identified as follows:

- UNM Medical Plan (for health benefits – administered through Presbyterian Health Plan, and administered through Lovelace Insurance Company)
- Delta Dental (for dental benefits – administered through Delta Dental)
- Flexible Healthcare Spending Benefit (for flexible spending accounts – administered through Stanley, Hunt, Dupree & Rhine, Inc. ("SHDR"))
- Prescription Drugs (administered and managed by Express Scripts, Inc.)

(the above-referenced health benefit plans shall be referred to collectively in this Policy as the "Health Plans"). Members of the University's workforce who work to administer the Health Plans may have access to the individually identifiable health information of Health Plans participants on behalf of the Health Plans itself or on behalf of the University, as plan sponsor, for the administrative functions of the Health Plans.

The Health Insurance Portability & Accountability Act and its implementing regulations ("HIPAA") restrict the Plan Sponsor's ability to use and disclose protected health information ("PHI").

> ***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; 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.

All employees covered by the Health Plans have received the Health Plans' Notice of Privacy Practices that includes specific individual rights and the duties required by the regulations. The University has always had a strong commitment to employee privacy and confidentiality; HIPAA is just one more dimension of this commitment. In fact, many HIPAA requirements are already in place.

2. Plan's Responsibilities as a Covered Entity

2.1 Privacy Officer and Contact Person.

The Privacy Officer for the University is:

Sophia Collaros, Privacy Officer
University of New Mexico
1 University of New Mexico
MSC 08 4760
Albuquerque, NM 87131
(505) 272-1493

The Privacy Officer is responsible for the development and implementation of the University's Health Plans' privacy policies and procedures. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI and shall be

able to provide further information about matters covered by the Health Plans' Notice of Privacy Practices (NPP).

2.2 Workforce Training

It is the University's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures (all employees with access and employees reasonably likely to have access to PHI, shall each be referred to in this Policy as a "Responsible Employee," and, collectively, the "Responsible Employees"). The Privacy Officer is charged with developing training schedules and programs so workforce members receive the training necessary and appropriate to permit them to carry out their functions within the Health Plans.

2.3 Procedural, Electronic and Physical Safeguards

The University has established, on behalf of the Health Plans, appropriate procedural, electronic, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. The University conducts periodic meetings with vendors and Business Associates to share privacy concerns, and to review procedures and security issues. Contracted service providers and other entities with whom the Health Plans must exchange information to conduct business are required to sign a Business Associate Agreement through which that entity must agree to maintain the privacy of confidential information according to the requirements of applicable privacy laws and the Health Plans' Privacy Policies & Procedures.

2.3.1 Procedural Safeguards. All employees are accountable for, and required to maintain, the confidentiality of personal information and must follow the University's policies established to secure such information. The University conducts ongoing employee training concerning privacy and compliance issues. Employees may require sufficient information to identify that an individual has a legitimate need for this information before it is provided. Responsible Employees must sign the University's Confidentiality Agreement which makes it clear that unauthorized or inappropriate disclosure of confidential information may be grounds for disciplinary action up to and including termination.

2.3.2 Electronic Safeguards. The University has safeguards in place concerning the storage and retrieval of electronic information. Access to electronic information is provided only to those with a legitimate need to know, and the information provided is limited to the minimum necessary for the stated purpose. Computer information is accessible only through individual sign-on and personal passwords that are periodically changed to maintain security.

All computer files and databases containing PHI received, created, or maintained by the Health Plans in electronic form, which require access by more than one Responsible Employee or which may be accessed by a Business Associate or a participant will be maintained on a secure network.

Upon termination of a Responsible Employee's employment, or upon a change or reassignment of an employee whose job functions have changed so that he or she is no longer a Responsible Employee, he or she shall be removed from authorized entry into any files, databases and other PHI maintained in electronic form. Such terminations shall be reported to the relevant University information technology system operations office who will adjust such former Responsible Employee's access to electronic PHI accordingly.

Any outside entity (including Business Associates) retained to perform information systems services will not be permitted access to any files, databases and other PHI in electronic form, except as necessary. The relevant University information technology system operations office will approve and grant such access. Business Associates must take reasonable steps to ensure

that third-party contractors retained by the Business Associates to perform information systems services will not be permitted access to the Health Plans' PHI, except as necessary. Business Associates must take reasonable steps to supervise third party contractors when such contractors have access to the Health Plans s' PHI.

2.3.3 Physical Safeguards. Original documents and copies of documents containing confidential health or medical information are retained in a locked room in the Benefit's Office for a period of not less than six (6) years and subsequently shredded or returned to the covered person as appropriate. Discarded documents are placed in a secure shred console until they are shredded. PHI must not be visible when a Responsible Employee is away from his or her work area for a significant amount of time. If a Responsible Employee shares a work area with someone who is not a Responsible Employee, PHI maintained in physical form must be stored in a locked filing cabinet, office or similar repository dedicated to the storage of PHI. The Privacy Officer will monitor the Responsible Employees authorized to access such stored PHI in the normal course of their duties. A Responsible Employee may access a filing cabinet, office, or repository in which PHI is stored only if he or she is authorized to do so or is acting under the direct supervision of such a Responsible Employee.

2.3.4 Remote Access to PHI. A Responsible Employee or Business Associate who remotely accesses PHI is subject to all applicable requirements of this Privacy Policy. PHI may be remotely accessed electronically using a secured, encrypted connection that meets University standards. Responsible Employees and Business Associates who work remotely must restrict access to the area in which PHI is used, maintained, or stored. When not required to be readily available for use by a Responsible Employee or Business Associate, PHI maintained in physical form must be reasonably secured and must not be left in open view for any significant period of time. The Responsible Employee or Business Associate must take steps to ensure that PHI used and stored in the off-site work area cannot be accessed by others, including the Responsible Employee's or Business Associate's family members.

All PHI received or created by a Responsible Employee or Business Associate who is working remotely must be secured and accounted for consistent with this Privacy Policy and the University's computer use and electronic communications policies. If a Responsible Employee or Business Associate creates or receives any PHI that is part of a designated record set (as described in Section 4.1 of this Policy), such PHI must be stored and maintained on the appropriate system or on the University's or the Business Associate's premises, in accordance with Section 2.3.3 above.

2.4 Privacy Notice

The University has developed a Notice of Privacy Practices in respect of the Health Plans. All employees covered by the Health Plans have received that Notice of Privacy Practices that includes specific individual rights and the duties required by the regulations. The Notice of Privacy Practices informs participants that the University will have access to PHI in connection with its plan administrative functions. The Notice of Privacy Practices is individually delivered to all participants:

- on an ongoing basis, at the time of an individual's enrollment in the Health Plans;
- within 60 days after a material change to the notice

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

2.5 Complaints.

The University's Privacy Officer will be the Health Plans' contact person for receiving complaints. The Privacy Officer is responsible for receiving privacy complaints about the Health Plans' privacy procedures and for handling such complaints. A copy of the form for lodging a complaint shall be provided to any participant in the Health Plans upon request.

2.6 Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy and/or HIPAA itself, or the Privacy and Security Rule Regulations promulgated thereunder will be imposed in accordance with the University's Policies on discipline, up to and including termination of employment.

2.7 Mitigation of Inadvertent Disclosure 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 policy and procedure. As a result, if an employee becomes aware of a disclosure of protected health information, either by an employee working to administer the Health Plans, a third party administrator/business associate or any subcontractor thereof, a third-party benefit manager/business associate or any subcontractor thereof, or other outside consultant/contractor, that is not in compliance with this HIPAA Policy and/or HIPAA itself, or the Privacy and Security Regulations promulgated thereunder, they should immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the Health Plans participant can be taken.

2.8 No Intimidation 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.

2.9 Plan Document

The Plan Document has been amended to include provisions describing the permitted and required uses and disclosures by the University for plan administrative purposes. Specifically, the Plan Document requires the University to:

- **2.9.1** Not use or disclose PHI other than as permitted or required by the Health Plans or as required by law.
- **2.9.2** Ensure that any agent, including a subcontractor, to whom it provides PHI received from the Health Plans, agrees to the same restrictions and conditions that apply to the University with respect to PHI.
- **2.9.3** Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the University.
- **2.9.4** Make available PHI to comply with HIPAA's right to access in accordance with 45 C.F.R. § 164.524.
- **2.9.5** Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526.
- **2.9.6** Make available the information required to provide and accounting of disclosure in accordance with 45 C.F.R. § 164.528.
- **2.9.7** Make its internal practices, books, and records relating to the use and disclosure of PHI received from the Health Plans available to the Secretary of the U.S. Department of

Health and Human Services for purposes of determining compliance by the Health Plans with HIPAA's privacy requirements.

2.9.8 Return or destroy all PHI received from the Health Plans 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.

2.9.9 Ensure that the adequate separation between Health Plans and the University (i.e., the "firewall"), required in 45 C.F.R. § 164.504(f)(2)(iii), is satisfied.

The Plan Document also certifies that the Plan Documents have been amended to include the above restrictions and that the University agrees to those restrictions and has provided adequate firewalls.

2.10 Documentation

The Health Plans' Privacy Policies & Procedures shall be documented and maintained for at least six (6) 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 Notice of Privacy Practices published in respect of the Health Plans, that Notice of Privacy Practices must be revised promptly and made available to Health Plans participants. Such change is effective only with respect to PHI created or received after the effective date of the notice.

The Plan Sponsor 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. The Plan must maintain such documentation for at least six years.

3. Policies on Use and Disclosure of PHI

3.1 Use and Disclosure Defined

The University will use and disclose PHI in connection with the Health Plans only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

> ***Use***. For information that is protected health information, use means the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Benefit and Employee Services Department of the Human Resources Division, or by a Business Associate (defined below) of the Plan.
>
> ***Disclosure.*** For information that is protected health information, disclosure means any release, transfer, provisions of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Division of Human Resources of the University.

3.2 Workforce Must Comply with the University's Policy and Procedures

All members of the University's workforce who have access to PHI (i.e., the Responsible Employees) in connection with the Health Plans must comply with this HIPAA Privacy Policy.

3.3 Access to PHI is limited to Responsible Employees

The University, as plan sponsor in respect of the Health Plans, shall allow the following University employees access to PHI:

3.3.1 Plan Administrator, the University's Vice President of Human Resources,
3.3.2 Benefits Office employees,
3.3.3 Privacy Officer and/or any Privacy Officer designee,
3.3.4 ITS Department employees that provide technical support for the Health Plans participant database and networks,
3.3.5 Office of University Counsel employees for the provision of legal advice and representation as to any matter or issue regarding the Health Plans or participant in the Health Plans, and

No other persons shall have access to PHI. These specified classes of employees shall only have access to and use PHI to the extent necessary to perform the plan administration functions that the University performs for the Health Plans.

3.4 Permitted Uses and Disclosures: Payment and Health Care Operations

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

Payment. Encompasses the various activities of health care providers to obtain payment or be reimbursed for their services, obtain premiums, fulfill their coverage responsibilities and provide benefits under the plan, and obtain or provide reimbursement for the provisions of health care. In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims;
- Risk adjustment;
- Billing and collection activities;
- Reviewing health care services for medical necessity, coverage, justification of charges and similar issues;
- Utilization review activities.

Health Care Operations. Health care operations are certain administrative, financial, legal and quality improvement activities of the Health Plans that are necessary to run its business and to support the functions of treatment and payment. These activities include:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- Reviewing the competence or qualifications of health care professionals, evaluating providers and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing or credentialing activities;
- Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
- conducting or arranging for medical review, legal and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the Health Plans, including development or improvement of methods of payment or coverage policies;
- Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets,

creating de- identified health information or a limited data set and fundraising for the benefit of the covered entity.

Because each of the Health Plans has one or more Third Party Administrators, virtually all of the day to day operations of the Health Plans fall into the "Payment" or "Health Care Operations" activities and do not require authorization from plan participants to take part in these activities on the Health Plans' behalf. Attached to this Policy as Appendix A and incorporated by reference is a description of the routine disclosures of PHI and to whom those disclosures will be made that will fall into the definition of "Payment" or "Health Care Operations."

3.5 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 such as long-term disability, workers' compensation, or life insurance, unless the Health Plans participant has provided an authorization for such use or disclosure or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

3.6 Mandatory Disclosures of PHI: to Individuals and HHS

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

3.6.1 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"; and

3.6.2 The disclosure is made to the Secretary of the U.S. Department of Health and Human Services, or his or her designee, for purposes of enforcing HIPAA.

3.7 Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI in connection with the Health Plans may be disclosed in the following situations without a Health Plans participant's authorization, when specific requirements are satisfied. Because such disclosures are highly unlikely as the University generally does not maintain such information in connection with the Health Plans, the University does not have procedures for such disclosures, the disclosures shall be in accordance with 45 C.F.R. § 164.502.

3.7.1 About victims of abuse, neglect or domestic violence;
3.7.2 For judicial and administrative proceedings;
3.7.3 For law enforcement purposes;
3.7.4 For public health activities;
3.7.5 For health oversight activities;
3.7.6 About decedents;
3.7.7 For cadaveric organ, eye or tissue donation purposes;
3.7.8 For certain limited research purposes;
3.7.9 For specialized government functions; and
3.7.10 That relate to workers' compensation programs.

3.8 Disclosures of PHI Pursuant to an Authorization

PHI in connection with the Health Plans may be disclosed for any purpose if the Health Plans participant provides an authorization that satisfies all of HIPAA's and applicable state law requirements for a valid and effective authorization. The University's **Authorization for the Use or Disclosure of Health Information Form** meets all of the HIPAA and applicable state law requirements. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

3.9 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 and disclosure. The "minimum-necessary" standard does not apply to any of the following:

3.9.1 Uses or disclosures made to the individual;
3.9.2 Uses or disclosures made pursuant to a valid authorization;
3.9.3 Disclosures made to the Secretary of U.S. Department of Health and Human Services or his or her designee;
3.9.4 Uses or disclosures required by law; and
3.9.5 Uses or disclosures required to comply with HIPAA.

See attached Appendix A for a description of disclosures that are routine and recurring. All other requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

3.10 Disclosures of PHI to Business Associates

Employees may disclose PHI in connection with the Health Plans to the Health Plans' business associates and allow the Health Plans' business associates to create or receive PHI on its behalf. The University has received signed Business Associate Agreements from each of the Health Plans' business associates assuring the Health Plans that each such business associate will appropriately safeguard the information.

3.11 Disclosures of De-Identified Information

The Health Plans may freely use and disclose de-identified health information of the Health Plans. 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. More specifically, "de-identified" information is defined as follows:

> ***De-identified Information*** – health information that does *not* include any of the following identifiers of the Individual or the Individual's relatives, employers, or household members: name; geographic subdivision smaller than a state (except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000); month and day of birth and other personal dates; telephone number; fax number; e-mail address; social security number; medical record number; health plan beneficiary number; account number; certificate or license number; vehicle identifier (including serial or license plate number); device identifier; serial number; Web Universal Resource Locator; Internet Protocol address number; biometric identifier; full face photographic image; or any other unique identifying number, characteristic, or code.
>
> Health information can also be considered "de-identified" if a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information and provided that the results of the analysis that justify such determination are documented by such person.

4. Policies on Individual Rights

4.1 Access to Protected Health Information

HIPAA gives Health Plans participants the right to access and obtain copies of their PHI that the Health Plans maintains in "designated record sets."

> ***Designated Record Set*** is a group of records maintained by or for the Plan Sponsor that includes:
>
> - The enrollment, payment and claims adjudication record of an individual maintained by or for the Health Plans; or
> - Other PHI used, in whole or in part, by or for the Health Plans to make coverage decisions about an individual

However, the University will not give Health Plans participants access to PHI records created in anticipation of a civil, criminal, or administrative action or proceeding. The University will also deny your request to inspect and copy Health Plans participant's PHI if a licensed health care professional hired by the Health Plans has determined that giving that participant the requested access is reasonably likely to endanger the life or physical safety of that participant or another individual or to cause substantial harm to that participant or another individual, or that the record makes references to another person (other than a health care provider), and that the requested access would likely cause substantial harm to the other person.

In the unlikely event that a Health Plans participant's request to inspect or copy his or her PHI is denied, that participant may have that decision reviewed. A different licensed health care professional chosen by the Health Plans will review the request and denial, and the University will comply with the health care professional's decision.

Health Plans participants may make a request to inspect or copy their PHI by completing the appropriate form available from the Benefits Department and sending it to the Benefits Department at the address listed in the Notice of Privacy Practices issued by the University in connection with the Health Plans. The University may charge a Health Plans participant a fee to cover the costs of copying, mailing or other supplies directly associated with the request. The Health Plans participant will be notified of any costs before any expenses are incurred.

4.2 Requests for Amendment to PHI

HIPAA also provides that participants in one or more of the Health Plans may request to have their PHI amended if a participant believes the information the Health Plans may have about that participant is incorrect or incomplete. Participants in the Health Plans have this right as long as their PHI is maintained by the Health Plans. The applicable third party administrator will correct any mistakes if the University (or one of its third party administrators) created the PHI or if the person or entity that originally created the PHI is no longer available to make the amendment.

Participants in the Health Plans may request amendments of their PHI by completing the appropriate form available from the University's Privacy Officer and sending it to the University's Privacy Officer at the address listed in Section 2.1 of this Policy. Evidence must be included to support the requested amendment because the University cannot amend PHI that the University and the Health Plans believe to be accurate and complete.

4.3 Accounting

HIPAA gives a participant in the Health Plans the right to obtain an accounting of certain disclosures of his or her own PHI. The accounting will not include (1) disclosures necessary to determine proper payment of benefits or to operate the Health Plans, (2) disclosures we make to you, (3) disclosures permitted by your authorization, (4) disclosures to friends or family members made in your presence or because of an emergency, or (5) disclosures for national security purposes. A participant's first request for an accounting within a 12-month period will be free. The Health Plans reserve the right to charge a participant for costs associated with providing additional accountings.

Accounting request forms are available from the University's Privacy Officer and a participant in the Health Plans may request such an accounting of disclosures from the University's Privacy Officer at the address listed in Section 2.1 of this Policy. When making a request, specify the time period for the accounting, which may not be longer than six years and may not include dates prior to April 14, 2003.

The Health Plans will respond to an accounting request within 60 days. The accounting will 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 that informs the individual of the basis for the disclosure.

4.4 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 that the Health Plans (or its third party administrators) call that participant only at work rather than at home.

Health Plans participants may request confidential/alternative communication of their PHI by completing an appropriate form available from the University's Benefits & Employee Services Department, UNM Human Resources Division (the "Benefits Department"). Participants in the Health Plans should send their written request for confidential/alternative communication to the Benefits Department. The Health Plans will honor all reasonable requests. Participants must specify how or where they wish to be contacted.

4.5 Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant in the Health Plans may request restrictions on the use and disclosure of the participant's PHI. For example, a participant in the Health Plans may ask the University to limit the scope of the participant's PHI disclosures to a case manager who is assigned to that participant for monitoring a chronic condition. Because the Health Plans use the participant's PHI only as necessary to pay benefits under the Health Plans, to administer the Health Plans, and to comply with the law, it may not be possible to agree to your request. *The law does not require the Health Plans to agree to a participant's request for restriction.* However, if the Health Plans do agree to the requested restriction or limitation, the Health Plans will honor the restriction until the participant agrees to terminate the restriction or until the Health Plans notify the participant that the Health Plans are terminating the restriction on a going-forward basis.

Restriction request forms are available from the University's Privacy Officer. Participants in the Health Plans may make a request for restriction on the use and disclosure of PHI to the University's Privacy Officer. Contact information for the University's Privacy Officer is set forth in Section 2.1 of this Policy. When making a request, a participant must specify: (1) the PHI requested to be limited; (2) how the participant wants the Health Plans to limit the use and/or disclosure of that PHI; and (3) to whom the participants wants the restrictions to apply.

APPENDIX A

Some disclosures of the Health Plans' PHI are made on a routine and recurring basis to individuals who have a legitimate need to know for healthcare operations purposes of the Health Plans. The Health Plans have determined that the following individuals have a legitimate need to receive PHI for the specified circumstance, and the Health Plans will implement and comply with the following policies and procedures that limit the PHI disclosed to the **minimum amount reasonably necessary** to achieve the purpose of the disclosure to these individuals for these circumstances:

Third-Party Administrators/Business Associates.

Presbyterian Health Plan, as one of the third-party administrators and Business Associate in respect of the UNM Medical Plan, shall have access to PHI that is available to the Plan Administrator of the UNM Medical Plan, in order to perform its duties relating to that Plan.

Lovelace Insurance Company, as one of the third-party administrators and Business Associate in respect of the UNM Medical Plan, shall have access to PHI that is available to the Plan Administrator of the UNM Medical Plan, in order to perform its duties relating to that Plan.

Delta Dental, as the third-party administrator and Business Associate in respect of the Delta Dental benefits plan, shall have access to PHI that is available to the Plan Administrator of the Delta Dental benefit plan, in order to perform its duties relating to that Plan.

Express Scripts, Inc., as the pharmacy benefit manager in respect of the University's prescription drug benefit plan, shall have access to PHI that is available to the Plan Administrator of the University's prescription drug benefit plan, in order to perform its duties relating to that Plan.

SHDR, as the third-party administrator of the University's Healthcare Flexible Spending Account plan, shall have access to PHI that is available to the Plan Administrator of the University's healthcare flexible spending account plan, in order to perform its duties relating to that Plan.

EBS/Atlanta, A Division of First Benecorp (USA), Inc., as the third-party administrator of the University's COBRA administrative services, shall have access to PHI that is available to the Plan Administrator of the University's various group health plans (Plans) subject to the Group Health Plan Provisions of the Consolidated Omnibus Budget Reconciliation Act of 1985 (COBRA), as subsequently amended, and the Health Insurance Portabiity and Accountability Act of 1996 (HIPAA), in order to perform its duties relating to those Plans.

Decisions on Claims and Appeals. The Plan Administrator, or the respective third party administrator, and/or arbitrator, who review claims decisions and/or claims appeals requiring the use of discretion, shall have access to and disclose that amount of PHI as they may deem necessary, in the exercise of discretion and professional judgment, to render a claims determination or decide an appeal.

Eligibility Determinations. For purposes of determinations of eligibility, the Plan Administrator, or the respective third party administrator, and/or arbitrator, who review eligibility decisions requiring the use of discretion, shall have access to all enrollment information of participants in the Health Plans and those individuals who have applied for coverage under the Health Plans.

Coverage Determinations. For purposes of determinations of coverage, the Plan Administrator, or the respective third party administrator, and/or arbitrator who review claims decisions and/or claims appeals

requiring the use of discretion, shall have access to an individual's claims file regarding the claim in question.

Plan Participants. For information purposes, Health Plans staff will release basic health plan enrollment information such as coverage levels and premium payments to the Plan Participant and any covered spouses or dependents.

Coordination of Benefits. For Coordination of Benefits purposes, the Plan Administrator, or the respective third-party administrator, shall have access to all enrollment information of the participants in the Health Plans who are the subject of the inquiry, as well as information regarding other coverage those participants may have.

Privacy & Security Officers. The University's Privacy & Security Officers shall have access to information regarding claims filed, appeals filed, eligibility, enrollment, termination, COBRA coverage and applications for coverage, as necessary to audit the day-to-day operations of the Health Plans in conjunction with the HIPAA Policies and Procedures. The University's Privacy & Security Officers shall have access to any PHI necessary to fulfill the responsibilities dictated in these policies.

Plan Auditor(s). The Auditor(s) of the University and of the Health Plansshall have information regarding claims filed, claims paid, eligibility, enrollment, termination, COBRA participants, COBRA premiums, participant contributions the health fund to audit the handling of funds related to the Health Plans as well as the assets of the Health Plans.

Plan Operations. The Plan Administrator or the respective third-party administrator, shall have access to all information needed to oversee and make decisions concerning operations of the Health Plans, including claims costs, administrative costs, and audit reports.

Plan Sponsor Audits. For auditing purposes, the University shall have access to claims information, as well as information regarding specific claims as are requested to assess the Health Plans' performance and review the costs of the Health Plans.

Underwriting. For underwriting purposes, the managing general underwriters from whom quotes are obtained shall have access to aggregate claims information, as well as such information regarding specific claims as are requested to determine the cause of unexpected claims that could influence the premium; however, whenever possible, this information shall be provided in de-identified form.

Utilization Review Companies. Any utilization companies used by the Health Plans shall have access to such medical records and medical information as they deem necessary to perform their duties related to pre-admission certification subject to the terms of the Business Associate Agreement between the utilization company and the Health Plans.

Case Management Companies. The applicable case manager of the case management company used by the Health Plans (or by the respective third-party administrator) shall have access to such medical records and medical information relative to the Covered Person(s) for whom they perform case management services as they deem necessary to perform their duties related to case management, subject to the terms of the Business Associate Agreement between the case management company and the Health Plans (or between the case management company and the respective third-party administrator).

Attorney(s). For purposes of providing legal services to the Health Plans, the Health Plans' attorneys (both the Office of University Counsel and any outside counsel retained by the University) shall have access to an individual's PHI that relates to the issues on which the attorneys advise the Health Plans.

Printing and Mailing Services. Any printing and mailing service used by the Health Plans shall have access to information necessary to be printed and mailed, to perform its duties for the Health Plans.

All other Disclosures. For all other disclosures, the University's Privacy Officer and/or the Privacy Officer's delegatee shall review each request for disclosure on an individual basis in accordance with the Health Plans' established criteria in these policies and procedures.