TABLE OF CONTENTS

University of Northern Colorado

HIPAA Policies and Procedures

Page #

University of Northern Colorado

HIPAA Policies and Procedures

The University of Northern Colorado ("University") has developed the following policies and procedures in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPPA). The privacy provisions of HIPAA apply to health information created or maintained by certain units or departments of the University.

The policies and procedures contained in this manual will be reviewed periodically to determine their appropriateness in order to comply with changes in laws, regulations and current practices.

All changes to this manual will be documented in the Appendix to this manual.

Development and Maintenance of HIPAA Policies and Procedures

The University president shall appoint one or more officials (Compliance, Privacy and Security) who may in turn appoint assistants for various functions or organizations. The Compliance Official will develop and/or oversee the development of policies and procedures that are in compliance with federal and state standards for the protection of the privacy and security of protected health information (PHI).

The Compliance Official may delegate this responsibility to a staff member.

The Compliance Official will remain accountable and responsible for all work product related to the development of all HIPAA policies and procedures contained in this manual produced by a designated staff member.

The Compliance Official will supervise the designated staff member in his/her development of HIPAA policies and procedures.

The University will maintain the policies and procedures in written form and will be referred to as University HIPAA policies and procedures manual. A written copy will be located at:

University of Northern Colorado	University Health Center	Speech and Audiology Clinic
Carter Hall – 4003	Cassidy Hall	Gunter Hall - 0330
Greeley, CO 80639	Greeley, CO 80639	Greeley, CO 80639

It will be available for any and all staff members to view during normal business hours.

For the purposes of this document the term "patient" shall include clients, students and faculty and staff.

Procedures for Updating HIPAA Policies and Procedures

It is the responsibility of the Compliance Official to:

- Monitor changes in federal and state law and regulations that may require changes in privacy policies and procedures
- Notify the President of the University of the issuance of new federal or state requirements and describe the need to modify policies and procedures, including the date by which revised policies and procedures must be implemented
- Take the initiative to develop new or revised policies and procedures as necessary to meet the requirements of new laws and regulations
- Identify any revisions that are needed in the privacy orientation and training program to reflect revised policies and procedures
- Revise the Notice of Privacy Practices to reflect the changes in the revised policies and procedures
- Document the changes made to the HIPAA Policies and Procedures Manual.

The effective date of a revised policy or procedure must not be earlier than the date on which the revised Notice of Privacy Practices is posted and made available to patients.

Approval of HIPAA Policies and Procedures

All policies and procedures must be approved by the Compliance Official of the University and reviewed by University legal counsel before such policies and procedures can be implemented.

The approval must be documented in the Appendix of this manual.

Communication and Implementation of Revised Policies and Procedures

New or revised HIPAA policies and procedures must to be communicated to the University staff through:

- The Compliance Official must send out an all staff notice announcing the adoption of the new or revised policies and indicate affected staff functions, new policy, its effective date, a copy of the new policy will be available for staff review

  and information on the dates, locations and times training on the new policy will take place

- The Compliance Official or a designated staff member must announce the adoption and effective date of the new policies at appropriate staff meetings

- The Compliance Official will send out specific notices to those staff members whose job responsibilities are directly affected by the new policies. This notice must contain the method of training and/or orientation dates and location, a copy

of the new policy and any background information that is available

- The revised policy will be distributed to all staff responsible for maintaining and updating copies of the HIPAA policies manual that are available to staff

Documentation and Record-Keeping

The Compliance Official or his or her delegee will establish policies and procedures for maintaining records of policy practices and procedures, written notifications, and enforcement actions taken.

Establishment of Record-Keeping Systems

The Compliance Official or his or her delegee will establish and oversee record-keeping systems to maintain the documentation required in this HIPAA Policies and Procedures Manual in compliance with the Health Insurance Portability and Accountability Act of 1996.

Maintenance of Written Records

The documentation to be maintained includes:

- The policies and procedures contained in this policy manual
- The Notice of Privacy Practices
- Signed acknowledgment of receipt of Notice of Privacy Practices
- Signed authorization forms
- Standard business associate clauses
- Records of disciplinary actions taken against staff members for violations of privacy policies and procedures
- Records of actions taken to enforce compliance with contract provisions by business associates
- Complaint forms received from patients or other individuals and associated written correspondence
- Records of privacy related education sessions and attendance rosters
- Approved requests for amendment or modification to patient information
- Approved requests for restricting uses and disclosures of PHI
- Approved requests for alternative methods for communicating with patients

Retention of Records and Documentation

All documentation of actions called for by other policies and procedures contained in this manual will be maintained for a minimum of six years from the date of its creation or the date when it last was in effect or changed, whichever is later.

Staff Roles and Responsibilities

The policies in this section establish the organizational roles, responsibility and accountability for the efforts of the University to safeguard information in compliance with federal and state standards for the protection of the privacy of health information.

Compliance Official

The Compliance Official oversees the University's compliance with all regulatory and governing agencies.

The University Compliance Official is responsible and accountable for the entire University's adherence to the policies and procedures contained in this manual.

The Compliance Official will:

- Designate the Security Official and the Privacy Official for the University
- Document the names of the Compliance Official, the Privacy Official, and the Security Official in the Appendix of this Manual
- Document all changes to the policies and procedures manual in the Appendix of this manual
- Maintain the HIPAA policies and procedures manual
- Insure employees of the University are educated with regards to HIPAA and the policies and procedures contained in this manual
- Insure all employees understand their roles and responsibilities with regards to HIPAA
- Review the policies and procedures contained in the manual for appropriateness every six months
- Document the review of the policies and procedures in the Appendix of this manual
- Limit staff member access to only information necessary to carry out their duties.
- Insure University legal counsel develops and or reviews specific language for all contracts that will extend state and federal privacy and security protections to any patient information created or accessed by a business associate (as defined in this manual)

The Compliance Official may assign the execution of any or all of these responsibilities to other qualified staff members or appropriate individuals but will be responsible for oversight and maintain responsibility and accountability for all duties and responsibilities outlined above.

Privacy Official

The Privacy Official is responsible for the development and implementation of policies and procedures to safeguard the privacy of patients' health information consistent with federal and state laws and regulations.

The specific responsibilities of the Privacy Official include:

- Developing privacy policies and procedures
- Developing and conducting training programs on privacy policies and procedures
- Responding to questions from staff and patients (including clients and others who may provide individually identifiable health information to University units or departments) concerning privacy policies and procedures
- Receiving complaints concerning the privacy practices described in the Notice of Privacy Practices
- Auditing compliance with privacy policies and procedures
- Investigating and correcting violations of privacy policies and procedures
- Designate a contact person or office responsible for providing further information and receiving complaints about privacy practices

The Privacy Official may assign the execution of any or all of these responsibilities to other qualified staff members or appropriate individuals, but will be responsible for oversight and maintain responsibility and accountability for all duties and responsibilities outlined above.

Security Official

The Security Official oversees and manages the development and implementation of the University's security policies, procedures, and technical measures.

The Security Official will

- Develop and implement policies and procedures that are consistent with federal and state security requirements
- Advise the management of information technology regarding the security requirements of federal and state law and with the policies and procedures to ensure compliance
- Conduct security training for all staff members and contractors
- Develop, implement, and test contingency plans
- Investigate security breaches
- Certify compliance of all security arrangements, including the technical capabilities of computer hardware and software, with the security policies of the practice and with federal security standard

The Security Official may assign the execution of any or all of these responsibilities to other qualified staff members or appropriate individuals, but will be responsible for oversight and maintain responsibility and accountability for all duties and responsibilities outlined above.

Information Technology Staff

Information Technology (IT) Staff members develop and maintain the University's information systems and technologies.

IT Staff members are responsible for:

- Meeting all systems security requirements that apply to the hardware, software, and databases they operate
- Establishing and communicating security safeguards required for protecting the data they manage
- Periodically reviewing and verifying that all users of the hardware, software, and databases they manage are authorized and comply with systems security safeguards
- Complying with and enforcing physical security requirements that apply to all hardware, software, and information storage media
- Reporting all security incidents to the Security Official or his or her designee, assisting in the investigation of incidents, and implementing corrective actions
- Working with all supervisors and users of information resources to ensure compliance with security policies and procedures, and the effective use of all security-related technologies (e.g., passwords, log-on/log-off procedures, etc.)
- Participating in the development, implementation, and testing of contingency plans

An IT Staff member may assign the execution of any or all of these responsibilities to other qualified staff members or business associates, but will be responsible for oversight and maintain responsibility and accountability for all duties and responsibilities outlined above.

Managers and Supervisors

Managers and supervisors are employees that oversee other employees or act as administrative heads to the University or one or more of the University's units of operation or business affairs.

Managers and supervisors are responsible for:

- Working with the Security Official to implement policies that will enable employees to access the information they need to perform their job duties
- Authorizing employees' appropriate access to job-related information resources
- Notifying the Security Official of all employee terminations, as well as changes to employee job functions, and terminations of agreements with contractors
- Increasing employee awareness of security policies and procedures
- Enforcing compliance with all security policies and procedures that apply to their staff
- Notifying the Security Official of all security breaches.
- Insuring staff member access of only the minimum necessary information to carry out their duties

A manager or supervisor may assign the execution of any or all of these responsibilities to other qualified staff members or appropriate individuals, but will be responsible for oversight and maintain responsibility and accountability for all duties and responsibilities outlined above.

Staff

Staff members are all employees, managers, supervisors, faculty, work-study students and graduate students of the University.

All staff members who generate or handle PHI must:

- Use and disclose protected health information only as authorized, necessary to carry out duties and in compliance with the University's Notice of Privacy Practices and/or Authorization for Use or Disclosure of Protected Health Information
- Conduct conversations in a manner that will avoid unintentional disclosures of patient health information
- Never intentionally use or disclose patient health information in a manner which violates state or federal regulations or the policies and procedures outlined in this manual
- Successfully complete security and privacy training
- Report suspected violations of a business associate's and/or contractor's contractual obligations
- Report any and all suspected violations of the policies and procedures established in this manual
- Safeguard the privacy and security of patient health information
- Protect the practice's technology resources, information, and data
- Attend required security training
- Use computer terminals and workstations, faxes, telephones, etc. in a manner that protects the security and privacy of patient health information
- Report all security breaches directly to the Security Official
- Maintain the confidentiality of their password

Authority and Responsibility of Individual Staff Members

All staff members who require routine access to protected health information to perform their job-related duties must identify be aware of:

- The job functions that require the use or disclosure of protected health information
- The types of protected health information that the position will use or disclose
- Any restrictions on the protected health information that the position can use or disclose
- The procedures that must be followed to use or disclose protected health information that is not routinely available to the position

Governing Body

The University President will be responsible for:

- Approving the policies and procedures contained in this manual prior to implementation
- Approving changes to the policies and procedures contained in this manual prior to implementation
- Receiving complaints and/or reports of suspected violations of the policies and procedures contained in this manual involving the Compliance Official, Privacy Official or Security Official

Business Associates

The University can disclose protected health information to a business associate, as defined below, and allow a business associate to create or receive protected health information on its behalf, provided that the business associate contractually agrees in writing, to appropriately safeguard the privacy and security of the information created, received or processed by the business associate.

A Business Associate is any person, business, organization, contractor, partner, subcontractor or employee thereof, with access to, receives or uses University created individually identifiable medical information or creates protected health information for the University, other than in the capacity of a staff member of the University or other arrangement involving the University, who on behalf of the University (or of an organized health care arrangement in which the University participates) performs, or assists in the performance of:

- A function or activity involving the use or disclosure of protected health information that is individually identifiable, including claims processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
- Any other function or activity regulated by Privacy Rule of the Health Insurance Portability Act of 1996; or
- Provides, other than in the capacity of a staff member of the University, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996), management, administrative, accreditation, or financial services to or for the University, or to or for an organized health care arrangement in which the University participates, where the provision of the service involves the disclosure of individually identifiable health information from the University or arrangement, or from another business associate of the University or arrangement, to the business associate

Responsibilities of Business Associates

All business associates with access to patient information or who receive, use or create protected health information from, with or for the University must:

- Sign a Confidentiality Agreement or contract containing satisfactory assurances with the University prior to receiving, using or creating protected health information
- Comply with the HIPAA policies and procedures established in the manual
- Include a chain-of-trust partner agreement in their contract with the University
- Require business associates to include chain-of-trust partner agreements in any agreements they enter into under a contract or agreement with the University

Business Associates Contract Requirements

All Business Associates must sign a HIPAA compliant contract with University after April 14, 2003, in a form which has been approved by the Colorado Attorney General or his or her designee.

Chain-of-Trust Agreements

All business contracts by and between the University's Business Associate and its contractors that provide access to patient information maintained by the University, or that involve the creation of patient information for use by the University, must include the following language:

> [Legal Name of Business Associate's contractor] agrees to comply with the HIPAA policies and procedures established in the University of Northern Colorado's HIPAA Policies and Procedures Manual, and with all state and federal privacy and security standards established under the Health Insurance Portability and Accountability Act of 1996. [Legal Name of business associate's contractor] further agrees to include this provision in any subcontract awarded pursuant to this contract.

Protected health information may be disclosed to business associates only if the University receives satisfactory assurances that the business associate will safeguard the privacy of the protected health information that it creates or receives.

Privacy

The University will maintain and establish administrative policies and procedures designed to ensure the privacy of protected health information.

Staff Training

This section establishes the responsibility for development and updating of staff training programs and materials on privacy policies and procedures. It also establishes the responsibility of all staff members to complete privacy training.

Content of Privacy Training Program for Staff

The Privacy Official or a staff member designated by the Privacy Official will develop a privacy policy orientation and training program.

The purpose of this program is to make sure that all staff members are familiar with the privacy policies and procedures that have been adopted by the University.

The training and orientation program will cover:

- The definition and identification of protected health information
- The Notice of Privacy Practices form that is provided to all patients
- Using and disclosing protected health information for treatment, payment, and health care operations
- Obtaining authorization for use and disclosure of protected information for purposes other than payment treatment or health care operations
- Operations; obtaining a signed acknowledgment of receipt of the University's Notice of Privacy Practices
- Patient privacy rights
- Procedures for handling suspected violations of privacy policies and procedures
- Penalties for violations of privacy policies and procedures
- Documentation required by the policies and procedures manual
- Summary of the University's privacy policies and procedures
- Opportunity to review the policy and procedure manual
- Opportunity to ask questions about the privacy policies and procedures of the University

Initial Privacy Orientation and Training

All staff members must complete the privacy policy orientation and training program during their probationary period.

- Completion of the privacy policy orientation and training program will be documented in the employee's personnel file by the Privacy Official,

or the staff member who conducts the training.
- Until staff members complete the privacy policy orientation and training program, their supervisors will closely monitor their use and disclosure of protected health information.
- Prior to the end of a staff member's probationary period, his or her supervisor should confirm that he or she has completed privacy training.

Training Staff on Revised Policies and Procedures

The Privacy Official or a staff member designated by the Privacy Official will develop training materials on new or revised privacy policies and procedures.

Procedures

- Staff whose job responsibilities are affected by a change in privacy policies and procedures must complete training on the revised policies and procedures
- Completion of training on revised policies and procedures will be documented in the employee's personnel file

Compliance and Sanctions

The University will establish and maintain appropriate policies and procedures for disciplinary actions and sanctions for employees and business associates whose actions are in direct conflict with the University HIPAA Policies and Procedures Manual.

Reporting of Suspected Violations of Privacy Policies and Procedures

All staff members must report possible violations of HIPAA policies and procedures to their supervisor. If the supervisor determines that a violation occurred, or that the situation warrants further investigation, the possible violation must be reported to the Privacy Official.

Under the following circumstances, potential violations should not be reported by a staff member to his or her supervisor:

- When the violation involves the staff member's supervisor, it should be reported directly to the Privacy Official
- When the violation involves the Privacy Official, the Security Official or the Compliance Official it should be reported to the President of the University
- If the violation involves the President of the University, it should be reported to the Privacy Official

Reportable offenses include use and disclosure of protected health information that may violate:

- The practices described in the Notice of Privacy Practices form
- Federal or state law

- The policies and procedures contained in this manual
- The University's compliance program
- A patient's authorization
- Unnecessary discussion of protected health information in public areas or in a location where the discussion might result in the disclosure of protected health information to unauthorized individuals

The staff member reporting a violation should briefly describe the possible violation in writing, or should arrange a meeting with the Privacy Official to discuss the possible violation.

Sanctions and Penalties

There are two types of violations of privacy policies and procedures:

- Technical violations that do not result in the inappropriate use or disclosure of protected health information
- Violations that do involve the inappropriate use or disclosure of protected health information

There also are two types of violations that involve use and disclosure:

- Unintentional or accidental uses or disclosures
- Intentional and deliberate uses and disclosures

The severity of penalties varies based on the type of violation. The most severe penalties apply to the intentional disclosure of protected health information in violation of policies and procedures. The least severe penalties apply to unintentional technical violations of policies that do not result in the disclosure of protected health information.

Examples of violations include, but are not limited to:

- Technical violations. When obtaining an authorization, a staff member fails to notice that the patient signed but did not date the authorization form. A change is made to the the policies and procedures manual and the staff is not notified of the changes
- Accidental disclosure. Information on two patients is accidentally mixed up, and the wrong information is faxed to third-party payors. Two coworkers are discussing a patient's request for a prescription refill in the hallway while another patient is walking by with the nurse
- Intentional disclosure. A staff member provides a drug company representative a list of patients with an identified medical condition without obtaining the patient's authorization for this disclosure. A staff member tells a friend of the patient the results the patient's HIV test over the telephone

Investigation of Potential Privacy Violations By Staff Members

Upon being notified of a potential violation of privacy policies and procedures by a staff member or patient the Privacy Official must:

- Review any documentation that has been prepared
- Meet with the staff member or patient who reported the possible violation
- Meet with the staff member(s) who may have violated the policies and procedures
- Determine what, if any, protected health information was used or disclosed
- Determine whether the use or disclosure violated policies and procedures
- Determine whether the violation was accidental or intentional
- Recommend to the staff member's supervisor the disciplinary action, if any, that should be taken
- Document the findings of the investigation and action taken

Sanctions and Penalties for Technical Violations

A staff member who commits a technical violation of privacy policies and procedures that does not result in any use or disclosure of protected health information will:

- Meet with his or her supervisor to review the policies and procedures that were violated
- Demonstrate to the satisfaction of the supervisor that he or she understands the policies and procedures that should be followed in similar circumstances

The violation will be documented in the staff member's personnel file.

A pattern of repeated technical violations, even if none result in the inappropriate use or disclosure of protected health information, may result in transfer to another position, suspension, or termination of the staff member.

Sanctions and Penalties for Unintentional Violations

A staff member who unintentionally uses or discloses protected health information in violation of the privacy policies and procedures will:

- Meet with his or her supervisor to review the use or disclosure of protected health information that violated the medical practice's policies and procedures or the staff member's authority to use or disclose information
- Demonstrate to the satisfaction of the supervisor that he or she understands the uses and disclosures that he or she is authorized to make under the practice's policies and procedures

The violation will be documented in the staff member's personnel file.

A pattern of repeated unauthorized use or disclosure of protected health information will result in transfer to another position, suspension, or termination of the staff member.

Sanctions and Penalties for Intentional Violations

The intentional violation of privacy policies and procedures may result in immediate suspension, pending further investigation and termination. Documentation of the investigation of the violation must show clear evidence that the disclosure of information was intentional and deliberate. That is, the staff member must have disclosed the information knowing that the disclosure violated the policies and procedures of the University.

If the staff member has previously disclosed the same or similar type of information under the same or similar circumstances, it will be presumed that the disclosure was intentional and deliberate.

Protection of Whistleblowers

No action shall be taken against a staff member who reports violation of privacy standards to the Secretary of the U.S. Department of HHS or to law enforcement agencies.

Documentation of Sanctions Brought Against Employees

The Privacy Official will document all actions taken to impose sanctions under policies and procedures in this manual. All actions taken to impose sanctions will be summarized in an Appendix of this manual. The summary shall include:

- A description of the violation and the documenting evidence
- A statement clarifying the nature of the violation, specifically indicating whether it was technical or involved the use or disclosure of protected health information, and whether the violation of policies was accidental or intentional
- A description of the sanction that was imposed

Such information will be placed in the employee's personnel file.

Duty of Staff to Report Contractual Breaches by Business Associates

If a staff member becomes aware of activities or practices by the business associate that violate its contractual obligations, it must be reported to the Privacy Official.

Investigation and Correction of Contractual Breaches

When the Privacy Official is notified that a business associate has violated a contractual provision related to the privacy of protected health information, he or she must implement the following procedure to correct the violation.

- The Privacy Official will contact the business associate and determine whether a contractual provision has been violated

- If a contract provision has been violated, the Privacy Official will identify steps to be taken by the contractor that will enable the contractor or the contractor's business associate to comply with contractual obligations to the University
- The Privacy Official will review the corrective action steps with the business associate and determine whether those steps or other measures suggested by the business associate will correct the violation. If an agreement can be reached, the corrective measures will be summarized in writing and sent to the business associate
- The Privacy Official will monitor the implementation of the corrective action measures by periodically contacting the business associate. The Privacy Official may discontinue monitoring the contract after receiving adequate assurances that the corrective measures have been implemented and that the contract provisions will be complied with in the future

If it is not possible to develop an acceptable corrective action plan, the Privacy Official shall implement the procedures established in the contract to terminate the contract.

Reporting of Contractual Breaches by Business Associates

When the Privacy Official is not able to correct violations of contractual obligations by a contractor, he or she should implement the following procedure.

- An alternative source for the services provided by the business associate should be identified
- The matter should be referred to the University's legal counsel with a request that formal action be taken to terminate the contract
- The business associate should be notified by the University's legal counsel that action will be taken to terminate the contract if the violation of contract provisions is not immediately corrected
- The status of the contract should be monitored by the Privacy Official and arrangements should be made to replace the business associate when the contract is formally terminated

If the contract cannot be terminated, the contract violation should be reported by legal counsel to the U.S. Department of HHS.

Privacy Policies and Procedures

Each unit or department of the University that handles individually identifiable health information will establish and maintain a supplementary policies and procedures manual dealing with its unique circumstances in accordance with local, state and federal privacy mandates.

Responsibility for Developing and Updating the Privacy Manual

The Privacy Official will develop policies and procedures that are reasonably designed to ensure compliance with federal and state standards for the protection of the privacy of health information. The Privacy Official may delegate this responsibility to a staff member, but such

delegation must be reflected in that staff member's job description and the Privacy Official will supervise the development of all privacy policies and procedures.

Procedures for Updating Privacy Policies and Procedures

It is the responsibility of the Privacy Official to:

- Monitor changes in federal and state law and regulations that may require changes in privacy policies and procedures
- Notify the President of the issuance of new federal or state requirements and describe the need to modify policies and procedures, including the date by which revised policies and procedures must be implemented
- Take the initiative to develop new or revised policies and procedures as necessary to meet the requirements of new laws and regulations
- Identify any revisions that are needed in the privacy orientation and training program to reflect revised policies and procedures
- Revise the Notice of Privacy Practices to reflect the changes in the revised policies and procedures

The effective date of a revised policy or procedure must not be earlier than the date on which the revised Notice of Privacy Practices is posted and made available to patients.

Approval of Policies And Procedures

All policies and procedures must be approved by the President of the University before such policies and procedures can be implemented.

Communication and Implementation of Revised Policies and Procedures

New or revised policies and procedures are to be communicated to staff through:

- An all-staff memorandum from the Privacy Official will announce the adoption of the new or revised policies and indicate affected staff functions. This memorandum should describe the new policy, indicate its effective date, and indicate the date on which the new policy will be available for staff review
- The Privacy Official or a designated representative will announce the adoption of the new policies at appropriate staff meetings
- A targeted memorandum will be circulated by the Privacy Official to those staff members whose job responsibilities are directly affected by the new policies. This memorandum should indicate whether training or orientation meetings or programs will be held, and whether background information on the new policy is available. A copy of the revised policy should be attached to the memorandum, or staff should be directed to consult the updated policy and procedure manual
- The revised policy will be distributed to all staff responsible for maintaining and updating copies of the policy manual

Documentation and Record-Keeping

The University will establish and maintain policies and procedures for maintaining records of policy practices and procedures, written notifications, and enforcement actions taken.

Establishment of Record-Keeping Systems

The Privacy Official or his or her designee will establish and oversee record-keeping systems to maintain the documentation required in this policy manual.

Maintenance of Written Records

The documentation to be maintained by each unit or department includes:

- The policies and procedures contained in this policy manual
- The Notice of Privacy Practices
- Signed acknowledgment forms
- Signed authorization forms

- Records of disciplinary actions taken against staff members for violations of privacy policies and procedures
- Records of actions taken to enforce compliance with contract provisions by business associates

- Complaint forms received from patients or other individuals and associated written correspondence

Storage of Records and Documentation

- Written policies and procedures, including updates will be maintained in this manual
- Changes to this manual will be recorded in the Appendix of this manual
- A copy of the University's Notice of Privacy Practices will be kept in an Appendix of this manual
- A copy of the University's Receipt of Acknowledgment of Notice of Privacy Practices form will be kept in an Appendix of this manual
- A copy of the University's Standard Authorization form will be kept in an Appendix of this manual
- A copy of the University's Standard Business Associate Contract will be kept in an Appendix of this manual
- Records of disciplinary actions taken against staff members for violations of privacy policies and procedures will be kept in the appropriate unit or department and logged in an Appendix to this manual and a copy of the documentation will be given to the Human Resources Department to be kept in the employee's personnel record

- Records of actions taken to enforce compliance with contract provisions by business associates will be recorded in an Appendix of this manual and a copy will be put in the business associate's file
- Complaint forms received from students, patients or other individuals and associated written correspondence will be kept in the Student Health Center and the Speech and Audiology Clinic and logged in an Appendix of this manual

Retention of Records and Documentation

All documentation of actions called for by other policies and procedures contained in this manual will be maintained for a minimum of six years from the date the information was created.

In the case of policies and procedures, the six-year retention period will be measured from the date of the most recent revision of the policy. In other words, when new policies are issued, the policies that are superseded should be retained for six years following the last day the policy was in effect.

Notice

The University will establish and maintain a Notice of Privacy Practices that is consistent with the Health Insurance Portability and Accountability Act of 1996 as well as any other local, state and federal regulations applying to privacy practices for the use and disclosure of protected health information.

Notice of Privacy Practices

Content of Notice of Privacy Practices

The Privacy Official or his or her delegee is responsible for developing the Notice of Privacy Practices.

The Notice of Privacy Practices must be written in language that patients of ordinary intelligence and education will be able to understand and included the following statement.

The following language must appear exactly as it is shown here and must be prominently displayed at the top of the notice:

> **THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.**

Uses and Disclosures

This section of the Notice must describe and give examples of the uses and disclosures for purposes of treatment, payment, and health care operations.

It must identify the legally mandated disclosures that may be made without the patient's authorization.

It must indicate that any other use or disclosure of protected health information requires written authorization by the patient, and that the patient has the right to revoke an authorization.

Additional Uses of Information

The uses and disclosures listed in this section must be specified if the University intends to use protected health information for any of the listed activities. This section can be merged with the previous section.

Note:

An additional use or disclosure that the regulations requires to be disclosed concerns disclosure of information to plan sponsors. This information is, however, relevant only to disclosures by a health insurance issuer (including an HMO) to a group health plan.

Individual rights

This section of the Notice of Privacy Practices must identify the rights of the patient under the federal privacy standards. These must include:

- The right to request restrictions of uses and disclosures
- The right to request restrictions on communication of health information
- The right to access protected health information
- The right to request an amendment of health information
- The right to adequate notice of privacy practices
- The right to receive a printed copy of the notice of privacy practices itself

The University's Duties

This section describes the duties of the University, specifically with respect to maintaining the privacy of protected health information, providing the Notice of Privacy Practices, and abiding by the terms of the privacy notice that is in effect when the patient receives it.

Right to Revise Privacy Practices

The notice must clearly state that the University reserves the right to modify its privacy practices and that should it do so, how the revised notice will be made available to patients.

Complaints

This section must outline the procedure for submitting complaints concerning the University’s privacy practices, or to report suspected violations of privacy rights.

It also must indicate that the University will not retaliate against the patient for submitting a complaint or reporting a suspected violation.

Contact Person

The Privacy Official listed in the Appendix to this manual shall be the contact person for any and all complaints concerning the University’s privacy practices.

Effective Date

This effective date of the Notice of Privacy Practices is April 14, 2003.

The effective date may not be earlier than the date on which the notice is printed and made available for distribution.

In the case of revisions to the notice, the effective date of the revised notice may not be earlier than the printing and release date of the revised notice. In other words, the policies described in the notice cannot go into effect before patients have been informed of the policies.

The current Notice of Privacy Practices may be found in an Appendix of this manual.

Providing the Notice of Privacy Practices to Patients

The University will make available to all patients of the various units of the University which create or augment protected health information a copy of the University's Notice of Privacy Practices.

The office administrator of the specific unit or department of the University will be responsible For providing a copy of the notice to all patients, no later than the first service delivery, following the date of this policy.

Requirements

- All patients will be provided a copy of the notice during their first contact following April 14, 2003, whether in-person in the office, via a telephone consultation, or through other electronic means such as email
- Any patient who requests a copy of the notice will be given a copy (a patient who receives a copy of the notice electronically may also request a printed copy)
- A copy of the notice will be posted in waiting areas
- The notice will be posted on the University's Web site
- An attempt will be made to obtain the patient's written acknowledgment of receipt of the University's Notice of Privacy Practices

Written Acknowledgment

The office administrator or an appropriately designated staff member, will request each patient, at their first appointment following April 14, 2003, to sign a written acknowledgment of the receipt of the University's Notice of Privacy Practices.

If the patient agrees to sign a copy of the University's Notice of Privacy Practices, the office administrator will provide the patient with a copy of the University's Notice of Privacy Practices and file the written acknowledgment of the receipt of the University's Notice of Privacy Practices in the patient's file.

If the patient does not wish to sign a copy of the University's Notice of Privacy Practices, the office administrator will provide the patient with a copy of the University's Notice of Privacy Practices and then document in the patient's file that the patient was given a copy and did not wish to sign. The good faith efforts made in trying to get the patient to sign the acknowledgment should include the date, time and name of person who dealt with the patient, as well as why the patient refused.

The University will not refuse to provide treatment to any patient based on their refusal to sign written acknowledgment of receipt of the University's Notice of Privacy Practices.

Use and Disclosure

The University will maintain and establish policies and procedures for the use and disclosure of protected health information that are compliant with state and federal privacy requirements and regulations.

Treatment, Payment and Healthcare Operations

Consent from the patient is not required to use and disclose patient protected health information for the purposes of treatment, payment and health care operations.

The University will use and disclose protected health information, as granted by regulatory permission, for treatment, payment and health care operations.

The University will obtain written authorization to use, disclose, receive, create or share patient protected health information for any purpose other than treatment, payment or healthcare operations.

Sharing Information Outside the University

When a provider who is not an employee of the University contacts a staff member and requests information for the purpose of treating a patient previously treated at the University, the staff member may provide information without restriction. It is not necessary for the patient to authorize the disclosure of protected health information that will be used for the purposes of treatment, payment or healthcare operations.

When disclosing information outside the University for the purposes of treatment, payment or healthcare operations, staff members should use the following procedure.

- Before disclosing information outside the University for the purposes of treatment, payment or healthcare operations, a staff member must verify the identity of the person making the request. In other words, the staff member must determine that the person making the request is, in fact, a health care professional who is requesting the information for the purpose of treatment. A staff member should obtain additional assurances sufficient to satisfy his or her professional judgment that the person requesting the information is a health care provider who will use the information for purposes of treatment
- Protected health information should be sent only to the verified business address of the provider requesting it

Faxing Information Outside of the University

The University will establish and maintain policies and procedures for faxing documents containing protected health information designed to safeguard the privacy and security of protected health information.

Documents containing protected health information will only be faxed if:

- The information is to be used to provide urgent patient care
- Mailing or couriering the information will not meet specific time deadlines
- Mailing or couriering the information will cost the University more than $25.00 US dollars
- Sending the information via fax will not violate any local, state or federal laws

Guidelines

If after reviewing University's rules for faxing, a staff member determines the necessity to fax information outside the University, the following guidelines should be followed (in addition to the normal policies and procedures for sharing information outside the University):

- The information sent must always be limited to the minimum necessary to meet the Immediate need of the requestor
- A cover sheet should always be used containing a copy of University's confidentiality statement
- The person providing the information (sending the fax) should verify the fax number and confirm receipt of the fax directly with the recipient of the protected health information

Confidentiality Statement

The University will maintain and establish a confidentiality statement to be used on documents containing protected health information.

A copy of the confidentiality statement will be kept in an Appendix of this manual.

Requesting Information from Outside the University

When a staff member requires information on a patient's health condition from another provider, he or she may request the information without restriction. The patient need not authorize this request.

The information requested must, however, be used for the purpose of evaluating the patient's medical condition or determining a course of treatment. A patient may have requested and been granted a restriction on the information that is to be used or disclosed to other providers. In this situation, the restriction must be honored.

Disclosure of Information to Family Members and Relatives

Protected health information concerning a patient may be disclosed in accordance with state and federal laws including the Family Educational Rights and Privacy Act (FERPA) to a spouse, child, other family member or relative who requires the information to assist in the patient's care and treatment, payment or health care operations.

- If the patient is able to, he or she must agree to the sharing of this information before it occurs
- If the patient is incapacitated, the medical staff members may exercise their professional judgment in determining when it is in the patient's best interests to disclose protected health information to a family member

The information that may be disclosed to the family member is limited to the information that is directly relevant to his or her involvement in the patient's care.

Various state laws govern the disclosure of information to a patient's parents including the following: Colorado Revised Statutes; Unfair methods of competition, C.R.S. 10-3-1104 et seq.; Confidentiality of health information, C. R. S. 10-16-423; Disclosure of Confidential Communications, C.R.S. 12-43-218; Theft of medical records or medical information, C.R.S. 18-4-412; Parentage information, C.R.S. 19-1-308; Artificial insemination, C.R.S. 19-4-106; Records of alcoholic & intoxicated persons, C.R.S. 25-1-312, Patient Records, C.R.S. 25-1-801, et seq.; Records of drug abusers C.R.S. 25-1-1108; Requests for release of information, C.R.S. 27-10-120.

Procedure

- If possible, disclosure of information to others should occur when the patient is present, or after the patient has agreed to the disclosure
- If the patient is present or available for consultation concerning the disclosure, he or she should be given an opportunity to object to the disclosure. If the patient objects to the disclosure, the information should not be disclosed
- If the patient is not present or available for consultation, or is incapable of agreeing or objecting to the disclosure, the attending physician or health care professional should exercise his or her best professional judgment to determine whether disclosure is in the best interest of the patient
- If the patient agrees to the disclosure or the disclosure is determined to be in the best interest of the patient, only that information that is directly relevant to the family member's involvement in the patient's care should be disclosed

Disclosure of Patient Information to Public Health Agencies

Certain information may be reported to the local and Colorado Department of Health as required
by law whether or not the patient authorizes the disclosure, including, but not limited to:

- Information required when compiling vital statistics (births and deaths)
- Information on communicable diseases

Mandatory Reporting of Child Abuse and Neglect

The University will report cases of suspected child abuse or neglect to appropriate County or State agencies as required by law even if the patient does not consent or authorize the disclosure. Staff must limit disclosure only to the types of information that must be disclosed pursuant to C.R.S. 19-3-304 (Persons required to report child abuse or neglect) and C.R.S. 19-3-305 (Required report of post mortem investigation).

The University will, as required by local, state and federal mandate, inform the patient and/or patient's guardian when a report of abuse, neglect, or domestic violence has been made.

Mandatory Reporting of Abuse, Neglect, and Domestic Violence

The University will report cases of suspected abuse, neglect, or domestic violence to appropriate County or State agencies as required by law even if the patient does not authorize the disclosure. In some cases, the University may not ask for the patient's authorization prior to the disclosure. Only the types of information that are required by law will be disclosed. See C.R.S. 12-36-125 (Injuries reported, penalty for failure to report – immunity from liability).

The University will, as required by local, state and federal mandate, inform the patient when a report of suspected abuse, neglect, or domestic violence has been made. Except when the staff in the exercise of professional judgment determines that informing the individual would place the individual at risk of serious harm or the practice would be informing the personal representative, and the staff believes the personal representative is the one responsible for the abuse or neglect.

Non-mandatory Reporting of Abuse, Neglect, and Domestic Violence

Staff may report cases of suspected child abuse or neglect to the appropriate County or State agencies without the agreement of the patient if the following criteria are met:

- The patient's physician believes that the report may prevent serious injury to the patient or others
- The disclosure is permitted under federal or state law

Staff members are to disclose only that information that is permitted by law to be disclosed.

The University will, as required by local, state and federal mandate, inform the patient when a report of suspected abuse, neglect, or domestic violence has been made.

Informing Patients of Disclosures

When protected health information is disclosed to a State or County agency**:**

- In accordance with local, state and federal mandate, the University will inform the patient of the disclosure unless the patient's physician or health care professional

believes that informing the patient may lead to serious harm for the patient or another person
- If the patient cannot be informed, the patient's personal representative must be informed of the disclosure unless the patient's physician or health care professional believes that informing the representative may lead to serious harm for the patient or another person

Disclosure of Patient Information to Law Enforcement

Agencies

Staff may disclose protected health information requested by law enforcement agencies without obtaining the patient's authorization.

Procedures

- Staff should refer requests for protected health information that are received from law enforcement agencies to the Privacy Official
- The Privacy Official will review requests for protected health information and obtain a legal opinion if he or she believes one is necessary before approving the disclosure of the requested information

The University will, as required by local, state and federal mandate, inform the patient when a disclosure is made to law enforcement agencies.

Disclosure of Patient Information to Oversight Agencies

Staff may disclose protected health information to government agencies such as the Colorado Department of Health**,** which are responsible for administering public health programs such as Medicare and Medicaid, and for licensing providers, conducting audits, and other purposes related to the oversight of the health system.

Procedures

- Staff should refer requests for protected health information received from oversight agencies, such as those mentioned above, to the Privacy Official
- The Privacy Official will review requests for protected health information and obtain a legal opinion if he or she believes one is necessary before approving the disclosure of the requested information

The University will, as required by local, state and federal mandate, inform the patient when a disclosure is made to oversight agencies.

Disclosures Related to Judicial and Legal Actions

Staff may disclose protected health information for use in a legal proceeding under the following circumstances:

- The information has been requested in a court order or an order of an administrative tribunal
- The information has been requested by means of a subpoena, discovery request, or other legal process

Before responding to the request, efforts should be made to ensure that only the minimum protected health information that is specifically requested is disclosed and that appropriate assurances are obtained as required by this manual.

The University will, as required by local, state and federal mandate, inform the patient when a disclosure is made for use in a legal proceeding.

Procedures

- Unless a request is referred by the Privacy Official, staff should refer requests for protected health information from law enforcement agencies to the Privacy Official
- The Privacy Official will notify and seek guidance from University legal counsel on how to respond to the request
- Before responding, the Privacy Official will obtain the assurances as required by this policies and procedures manual

Marketing

The University will maintain and establish policies and procedures for the use and disclosure of protected health information in marketing activities.

Marketing Communications

Marketing is defined as "to make a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service."

The University will obtain written authorization from the patient or the patient's representative to use his or her protected health information for marketing purposes except as outlined in this manual (and permissible by local, state and federal regulations).

If the marketing will result in direct or indirect remuneration to the University, a statement addressing the remuneration must be included in the authorization form.

Communications That Do Not Require Authorization

The following types of communications do not require authorization when they either are made orally or in writing and the University will receive no monetary compensation from an outside party as a result of the marketing communication and/or relationship:

- Communications to individuals about participating providers and health plans in a network, services offered by a provider, or benefits covered by a health plan
- Communications with a patient about the patient's treatment
- Communications about case management or care coordination; or directions or recommendations for alternative treatments, therapies, health care providers, or treatment settings

Marketing Communications That Do Not Require Authorization

The University may make a marketing communication in a face-to-face encounter with the individual, or that involves products or services of only nominal value, without requiring an authorization. For example, providing sample products during a face-to-face communication, or to distributing calendars, pens, and the like, that displays the name of a product or provider.
A promotional giveaway will be considered of nominal value if is not worth more than five ($5) dollars.

Marketing Communications That Require Authorization

The University will obtain written authorization from the patient or the patient's representative prior to any communication being sent to the patient or the patient's representative, for the purpose of encouraging them to purchase or use a product or service or any other purpose not specifically permissible by local, state and feral regulations without authorization.

The University will obtain written authorization from the patient or the patient's representative prior to the University disclosing, releasing or selling the patient's information to a third party for marketing purpose or any reason other than treatment, payment or healthcare operations.

Fundraising

The following information may be used to support efforts to raise funds that directly benefit the medical units of the University without obtaining the patient's authorization:

- Demographic information describing the individual (i.e., date of birth, sex, marital status, address, and other non-clinical information that describes the patient)
- The dates on which the patient received health care services from the medical practice

Other protected health information may not be used in fundraising activities without authorization by the patient. That is, the patient's authorization is required for the use of any protected health information except demographic information and dates of service.

Fundraising appeals sent to individuals must include the following paragraph describing how the individual may opt-out of further fund-raising communications:

> To be removed from future fundraising appeals, please call: [###-###-#### ext. ###] and ask to be removed from our fundraising mailing list.

A fundraising mailing list will be maintained by the administrator responsible for fund-raising**.** When a patient asks to be removed from the mailing list, a reasonable effort will be made to accommodate this request. Protected health information may not be used to support fundraising on behalf of other organizations (that is, for raising funds that do not benefit the University directly) without the patient's authorization.

Other Disclosure Situations

Disclosure of Information for the Purpose of Cadaveric Organ Donation

Following the death of a patient, a medical practitioner may disclose protected health information to an organ procurement organization such as an eye bank or tissue bank without the patient's prior authorization, and without obtaining the authorization of the patient's representative.

Staff may not disclose this information if a patient or the patient's representative has indicated that he or she does not want to donate organs or tissue, of if the patient has imposed a restriction on the disclosure of protected health information for this purpose.

Disclosure of Information to Coroners and Medical Examiners

Staff may disclose protected health information without the patient's authorization to a coroner
or medical examiner who requests the information for the following purposes:

- Identification of a deceased person
- Determination of the cause of death
- Other purposes specified in state or federal law

Procedures

- The credentials of the coroner or medical examiner making the request should be verified.
  If the request is made in person, staff should ask to be shown and official identification. If the request is made by telephone, staff should ask that the request be submitted in writing and should obtain the official address to which information should be sent.
- Staff should confirm that the information is being requested by the coroner or medical

examiner for use in establishing the identity of a deceased person or determining the cause of death.
- The requested information should only be sent to the official address of the coroner or medical examiner.

Disclosure of Information to Funeral Directors

The University may disclose protected health information that a funeral director requests for the purpose of preparing a body for burial or cremation.

Staff should attempt to obtain the permission of the patient's representative before disclosing requested information, but permission is not required.

Only the information that a funeral director is entitled to request under state laws should be disclosed.

Procedures

- The funeral director should be asked to submit a request for the specific information that is required in writing. This request may be faxed, but should identify the funeral director by name and address
- An attempt should be made to contact the patient's representative or a close family member (spouse, child, or other family member) or close personal friend who has been involved in the patient's treatment for permission to disclose the requested information
- The information that has been requested should only be sent to the business address of the funeral director

Disclosure to Avert a Threat to Health or Safety

A staff member may disclose protected health information without the authorization of the patient if, in his or her professional judgment and in good faith, such disclosure is necessary to reduce a serious and imminent threat to the health and safety of a person or the public.

- Information may be disclosed only to a person who is able, in the judgment of the staff member, to prevent or lessen the threat
- If the patient has threatened to harm or injure another person or persons, that threat may be disclosed to the person(s) identified by the patient as the target(s)
- If the patient has admitted that he or she has participated in a violent crime, that admission may be disclosed to law enforcement agencies
- If the staff member has reason to believe, based on all circumstances, that the patient has escaped from a correctional facility or lawful custody, the staff member may disclose that belief to law enforcement agencies

Staff members may not disclose information related to participation in a violent crime if that information is learned in the course of treatment, counseling, or therapy for a

propensity to engage in the criminal conduct, or if the patient has disclosed criminal activity while requesting referral for treatment, counseling, or therapy of such a propensity.

Disclosure to Disaster Relief Agencies

Information on a patient's location, medical condition, or death may be disclosed to disaster relief organizations such as the Red Cross and other public or private organizations.

Disclosure of Protected Health Information After Death

The protected health information of a deceased individual will be handled according to the policies and procedures applied to the protected health information of living patients. The death of a patient does not reduce the privacy protections that his or her protected health information will receive.

Authorization

Authorization refers to a specific permission to use or disclose protected health information for a specified purpose other than treatment, payment or healthcare operations. The University
will obtain valid written authorization prior to any use and/or disclosure of protected health information for purposes other than treatment, payment or healthcare operations.

Examples of uses and disclosures for which authorization would be required include:

- Providing camp or sports physicals or medical examinations required for participation in athletic activities
- Development of condition-specific mailing lists for marketing campaigns
- Participation in medical research and clinical trials

Elements of a Valid Authorization

The following elements are required for all authorizations:

- Description of the information to be used or disclosed
- Identification of the person or class of persons authorized to make the requested use or disclosure
- Identification of the person or class of persons authorized to receive the use or disclosure
- An expiration date or event
- Description of each purpose of the use or disclosure
- Signature of the individual and date
- If signed by a personal representative, a description of his/her authority to act for the individual
- Statement that the individual may revoke the authorization in writing
- Statement that treatment, payment, enrollment in a health plan, or eligibility for benefits may not be conditioned on obtaining an authorization if the conditioning is prohibited by the Privacy Rule or, if conditioning is permitted, a statement about the consequences of refusing to sign
- A statement about the potential for the protected health information to be re-disclosed by the recipient

The University will use a standard authorization for all authorizations except authorizations for psychotherapy notes and authorizations which condition treatment.

Obtaining Authorization

When protected health information will be used or disclosed for a purpose other than treatment, payment or healthcare operations, the patient's authorization must be obtained.

It is the responsibility of the staff person who wishes to use or disclose the information to initiate the procedure to obtain the patient's authorization.

Procedures

- The staff member requesting the authorization should obtain an authorization form and complete the sections describing the information to be used or disclosed, the purposes of the use or disclosure, the persons who will use or disclose the information; and the persons to whom the information will be disclosed
- The staff member or a person designated by the staff member should review the authorization request with the patient
- The patient may request restrictions on the use and disclosure of protected health information. The staff member requesting the authorization should consider these requests and may, at his or her discretion, accept or reject them. Those restrictions that are accepted should be clearly noted on the authorization form.
- The patient should sign and date the authorization form
- The signed and dated authorization form should be placed in the patient's record

Patients' Refusal to Sign an Authorization Form

A patient who refuses to authorize a specific use or disclosure may not be refused treatment except under the following circumstances:

- The treatment is available only to participants in a research study (provision of research-related treatment can be conditioned on provision of an authorization for use or disclosure of personal health information for such research)
- The provision of health care is solely for the purpose of creating personal health information for disclosure to a 3rd party

Procedure

- When a patient refuses to sign an authorization, the staff member should determine whether the request involves information included in either of the two categories listed above
- If the authorization is for use and disclosure of information for purposes of research-related treatment, the patient should be told that the treatment is available only to participants in a study, and that participants must authorize use and disclosure of their information in the study
- If the authorization involves a request for information from another organization, it should be explained to the patient that the services will not be provided unless disclosure is authorized
- If the patient continues to refuse to sign the authorization, the persons requiring the authorization should be notified of the patient's refusal

Revoking Authorization for Use or Disclosure

A patient may revoke an authorization at any time. The revocation must be in writing and must be attached to the related authorization.

Procedure

- A patient who indicates that he or she wants to revoke an authorization should be given an authorization revocation form
- The staff member who sought the original authorization, if he or she is available, or another staff member should explain to the patient that revoking the authorization will not affect any use or disclosure of information that has already occurred
- The patient should sign and date the revocation form
- The revocation form should be appended to the authorization and included in the patient's records

Requests for Restrictions

Patients may request restrictions on use and disclosure of protected health information.

The University must review and consider these patient requests before deciding to accept or reject them. The University is not required to accept them. The University should accept a request for a restriction on the uses and disclosures if they meet the following:

- The request will not impede treatment, payment, or healthcare operations
- The restrictions will not interfere with the purpose for which an authorization is being sought
- The patient has valid reasons for requesting the restrictions, in the judgment of the patient's physician or health care professional

Once the University accepts requested restrictions, the restrictions must be honored unless doing so would interfere with emergency treatment. For example, if the patient who requested the restriction is in need of emergency treatment and the restricted personal health information is needed to provide the treatment, the University may use or disclose the personal health information.

All restrictions to which the University agrees must be documented and maintained for at least six years.

A restriction on the disclosure of information that a patient requests and that the University agrees to does not prevent the University from disclosing information that is mandated by law and that does not ever require the patient's consent or authorization.

Procedure

- A patient may request a restriction
- The request should be reviewed by the Privacy Official or by a staff member designated by the Privacy Official to determine whether the requested restriction would impede the use of information for treatment, payment, or health care operations
- The Privacy Official**,** or the designated staff member should ask the patient to explain why he or she is seeking the restriction

- The restriction should be agreed to if, in the judgment of the Privacy Official or his or her designee, it will meet the requirements set out in this policy
- If the request is agreed to, it should be documented by the Privacy Official or by the staff member designated by the Privacy Official

Termination of Restrictions on Use and Disclosure

The University may terminate a restriction on the use and disclosure of protected health information to which it has agreed.

Patients must be notified of any termination of a restriction and must be given an opportunity to agree or disagree with the termination.

Regardless of whether the patient agrees to the termination or not, information collected after the University informs the patient of the termination may be used or disclosed as though the restriction had never been accepted.

The termination of a restriction must be attached to the authorization form in which the restriction appears.

Procedure

- A staff member who wishes to terminate a restriction should contact the Privacy Official or his or her designee and discuss the need for the termination.
- The termination request should be approved if the continuation of the restriction would substantially impede treatment, payment, or the day to day operation of the practice.
- The staff member should contact the patient to discuss the need for the termination and to seek his or her agreement.
- If the patient agrees to end the restriction, he or she should sign a statement to that effect. If the patient is not available to sign a written statement, his or her oral agreement should be noted, signed, and dated by the staff member who discussed the termination with the patient.
- The termination of the restriction should be attached to the consent or authorization form in which the restriction appears.

Patient Requests for Confidential Communication

Staff members must accommodate a patient's reasonable request for confidential communication if the following criteria are met:

- The patient provides an alternative address or telephone number at which he or she may be contacted
- The request can be accommodated without limiting the ability of the University to submit claims to the patient's health plan

If the request for confidential communication will prevent the University from submitting

claims to the patient's health plan, the request will be accommodated only if the patient identifies another method of paying for services provided by the University.

Requests for confidential communications must be made in writing. The patient must submit a written request directly to the University. The staff member receiving the request may not require the patient to explain why he or she wants to receive confidential communications.

Procedure

- When a patient requests confidential communication of protected health information (for example, the results of diagnostic tests), the staff member to whom the request is made should tell the patient that the request must be made in writing and explain the conditions that must be met before the request will be granted

- The patient should be given a confidential communication request form by the staff member to whom the request is made or by a staff member he or she identifies. The patient should be informed that his or her request will be accommodated if he or she provides an alternative means of making confidential communications. For example, the patient should provide a telephone number at which messages to contact the provider can be left. No method of contacting the patient that prevents a staff member from identifying both the patient and the practice will be considered acceptable. The request for confidential communication should be documented in the patient's record

Access

The University will establish and maintain policies and procedures for providing access to protected health information.

Personal Representative

A personal representative may act on behalf of the patient for the purpose of:

- authorizing use and disclosure of protected health information
- receiving information that otherwise would be sent to the patient

Designation of a Personal Representative

A personal representative may be the spouse, adult child, or other member of the patient's family. A personal representative also may be a close personal friend, or any individual, with power of attorney or other legally recognized authority to make medical decisions on behalf of the patient if he or she is incapacitated or otherwise unable to make decisions.

A person who is identified in the patient record as having medical power of attorney or other legal authority to act on behalf of the patient will be recognized as a personal representative.

A parent or legal guardian of a non- emancipated minor (an individual under the age of 18) will be recognized as a personal representative of that person.

Procedure

- A patient should be encouraged by the staff member of that department or unit to identify an individual or individuals who may act as his or her personal representative
- If a patient becomes incapacitated, a person accompanying the patient will be recognized as the patient's personal representative if he or she can present evidence of having medical power of attorney or other legally recognized authority to make medical decisions on behalf of the patient
- The parent or legal guardian of a non-emancipated minor will be recognized as the personal representative of a child, subject to the restrictions contained policies and procedures manual and state laws
- If a staff member is uncertain as to who is the appropriate personal representative, the matter shall be referred to the Privacy Official

Authority of Personal Representative

If a patient is incapacitated, a personal representative may sign any form (such authorization, revocation of authorization, and request for access to information), the uses of which are described in this privacy manual.

A personal representative may receive protected health information concerning the patient that he or she requires to perform his or her legal duties to the patient (for example, providing an informed consent to treatment, or for enforcing an advance directive concerning life support).

Refusal to Recognize Personal Representative

A staff member may refuse to disclose information to a person identified as a patient's personal representative if he or she believes that disclosing such information may endanger the patient.

Procedures

- A staff member who believes that disclosing information to a personal representative may endanger the patient should notify the Privacy Official
- Requests from the personal representative for information concerning the patient should be referred to the Privacy Official

The University does not have to treat someone as a personal representative if the staff has a reasonable belief that the individual has been or is subjected to domestic violence, abuse, neglect; or treating a person as a personal representative could endanger the individual; AND in the exercise of professional judgment decides it is not in the individual's best interest to recognize the person as the individual's personal representative.

Parental Access to Protected Health Information Concerning Children

A parent, guardian or other person recognized by state law as acting in loco parentis on behalf of a patient who is a non-emancipated minor will be recognized as the patient's personal representative.

A parent does not have the authority to act as a personal representative if:

- Parental consent to treatment is not required under state law and the minor has consented to treatment
- Parental consent to treatment is not required and the minor, a court, or another person who is authorized by law has consented to treatment
- A parent or legal guardian has agreed to an agreement of confidentiality between the provider and the minor

Generally, the University will require a parent or legal guardian's signature on any authorization forms for a minor patient unless the patient requests that his or her parents not be notified.

Procedure

- The Privacy Official should review any minor's request for confidentiality pertaining to the use or disclosure of protected health information that relates to a parent or guardian, to determine whether the request complies with state and federal laws

Patient Access to Health Information

This section of the privacy manual addresses a patient's request to inspect, copy, or amend his or her protected health information maintained by the University.

Patient Requests for Access to Protected Health Information

A patient or a patient's representative may inspect and obtain a copy of his or her information maintained in medical records or other information systems of the University.

Procedures

- A patient must submit a request to inspect or copy protected health information
- The request will be reviewed
- If the request is denied, the patient will be informed
- If the request is approved, the patient will be given access to the requested information

Submission of Request for Access to Protected Health Information

A patient must request an opportunity to inspect or copy his or her protected health information.

This policy does not address or prevent a physician or other health care professional from sharing the results of laboratory or other diagnostic tests with a patient or a patient's personal representative, or discussing the result of medical procedures. These communications related to treatment may be made orally or in writing at the discretion of the patient's physician or other health care professional.

This policy does not address or prevent other staff members from discussing or disclosing to the patient, orally or in writing, information related to the current status of claims that have been submitted to the patient's health plan.

Procedures

- When a patient or patient's representative orally requests access to information, he or she should be told that all requests to inspect or copy protected health

information must be submitted in writing. The patient should be referred to the administrator of the unit or department
- The staff member of that department or unit will give the patient or patient's representative a copy of the request form and explain the University's policies on allowing a patient to inspect his or her records
- Upon receipt of a request form, the staff member will forward the request to the Privacy Official for the review and processing

Review of Patient Requests for Access to Protected Health Information

The request for access to personal health information will be sent promptly to the Privacy Official. A copy of the request will be filed in the patient's records.

The Privacy Official will consider the restrictions on access listed below when determining whether to approve or deny the request to inspect or copy protected health information.

A decision to grant the patient or patient's personal representative permission to inspect or copy the requested information will be made within ten (10) of days of the date on which the request is submitted or within the time required by federal and state laws. The more stringent requirement prevails when there is a difference between the two.

Restrictions on Access

- Psychotherapy notes will not be made available to the patient unless approved by the treating therapist or designated successor
- Information compiled in anticipation of, or for use in, legal proceedings will not be made available to the patient or patient's legal representative unless required by law or court order
- Information that, by law, may not be disclosed to the patient will not be made available to the patient or patient's representative
- Information will not be made available if the patient's physician believes that it is likely to endanger the life or physical safety of the patient. This is a reviewable denial
- Information will not be made available if the patient's physician or other health care professional believes that access to the information is reasonably likely to cause substantial harm to a person other than the patient who is referenced in the patient's records. This is a reviewable denial
- Information will not be made available to a personal representative of the patient if the patient's physician or other health care professional believes that access to the information by the personal representative is reasonably likely to cause harm to the patient or to another person. This is a reviewable denial

Access will also be denied for personal health information that is subject to laws or regulations which prohibit access to of such information as a matter of law.

Procedures

- The Privacy Official will review the request to inspect or copy protected health information

- The Privacy Official will contact the patient's physician or other health care professional to determine if there are any reasons to restrict the patient's or patient representative's access to the information
- If the request is disapproved, wholly or in part, the patient will be notified according to University policy, as stated below
- If the request is approved the patient will be notified and arrangements made for the patient to inspect or copy the requested information

Denial of Requests

If a patient's request to inspect or copy protected health information is denied, wholly or in part, the patient will be contacted and given an opportunity to request a review of that decision. The review may be denied if it is prohibited by law.

A written explanation of the denial of a patient's request to inspect or copy protected health information will be provided to the patient by the Privacy Official or his or her designee. The following elements must be included in the denial:

- Written in plain language
- Reason for denial
- Statement of the individual's review rights
- Description of the complaint process
- Describe alternatives if available

If alternative information can be identified that may partially satisfy the patient's request, including a summary of the requested information, the communication should describe those alternatives.

Review of Decision to Deny Access

A patient or patient's representative whose request to inspect or copy protected health information is denied may request a review of that decision by a licensed health professional who was not involved in the decision to deny the request.

Procedures

- When the Privacy Official receives a copy of the denial notice indicating that the patient is requesting a review of the denial, he or she should forward the request to a licensed health professional who was not involved in the original denial and request that person review the decision

- The review should normally be completed within ten days. The Privacy Official will follow-up with the reviewing health professional if the review is not completed within 10 days of sending him or her the request
- The Privacy Official should communicate the result of the review to the patient

Inspection of Records

If the records must be retrieved from on-site storage, the patient should be notified that the requested information will be made available, generally within fifteen days of the date the request was made.

If, however, records must be retrieved from off-site storage, the records should be made available for inspection within twenty days of the submission of the request.

Communication of Decision

Approval of a patient's request to inspect or copy protected health information should be communicated to the patient or patient's representative.

The approval should specify the earliest date and time that the records will be available for copying.

Procedure

- The Privacy Official will determine the earliest date at which the requested information can be made available
- The Privacy Official or a designated staff person will notify the patient or patient’s representative

Arrangements for Inspection

Arrangements should be made to provide access to protected health information at a place and time convenient for the patient.

The patient must inspect the records on University premises. If this is not satisfactory to the patient, he or she should be given the option of having copies made and sent to an address that he or she specifies. However, the patient must pay for such copies as outlined in this policies and procedures manual.

Fees for Copying Personal Health Information

If the patient requests copies of personal health information maintained by the University, he or she will be charged a flat fee of $1.25 per page.

Amendment to Records

Request for Amendment

A patient may request amendment of the information describing him or her that is maintained by the University as part of the designated record sets listed below.

The patient must follow the procedures outlined in this manual when requesting amendment of information maintained by the University. A copy of the relevant policies and procedures must be provided to the patient by the University in order for the patient to comply.

Designated Record Sets

The designated record sets for which a patient may request amendment include:

- The patient's medical records
- The patient's billing records
- Other records that contain protected health information that is used to direct treatment
- Health Insurance claim information

Procedures

- The patient must request amendment of protected health information in writing. A form is available for this purpose and should be used if possible
- The request will be reviewed
- If the request is approved, the protected health information will be amended as provided for in this policies and procedures manual
- If the request is denied, the patient will be notified and offered the opportunity to submit a statement disagreeing with this decision that will be handled using the procedures in this policies and procedures manual

Procedures for Requesting Amendment

Requests to amend protected health information must be submitted in writing. Patients should use the patient information amendment form.

Procedures

- A patient who indicates to a staff member that he or she believes the information in his or her record is incorrect or incomplete should be given a patient information amendment form
- If the patient has questions about the form, he or she should be referred to the administrator of the department or unit

Action on Requests

The Privacy Official may deny a patient's request to amend records if the following criteria are met:

- The information to be amended was not created by the University, but was received from another entity
- The information to be amended is accurate and complete
- The information to be amended does not exist in the specified records
- The information to be amended is not available for inspection by the patient or patient's representative

Action must be completed on any request for amendment within ten days of receiving the request. If action cannot be completed within this time period, the University must notify the patient of the delay, including the reasons for the delay, and complete the review within a reasonable time after notification.

Procedures

- When a patient submits a patient information amendment form it will be forwarded to the Privacy Official
- The Privacy Official should contact the patient's physician or other health care professional or a staff member he or she designates and request a review of the requested amendments
- The physician or other health care professional or designated staff member should indicate which of the requested amendments should not be made because the information in the patient's record is accurate and complete
- The physician or other health care professional or designated staff member should then return the form to the Privacy Official
- The Privacy Official should review the form after it is returned by the patient’s physician or other health care professional and identify any information that should be amended
- The Privacy Official should initiate the procedures for amending protected health information specified by the policies and procedures in this manual
- The Privacy Official should prepare a response to the patient as required by the policies and procedures in this manual

Communication of Decision

After completing the review of a patient's request for amendment of protected health information, the Privacy Official will complete the patient information amendment form by indicating the disposition of each requested amendment.

A copy of the completed patient information amendment form will be sent to the patient along with any explanatory comments that the Privacy Official believes to be necessary.

The patient will be asked to submit the names and addresses of any organizations or individuals that he or she has reason to believe have received the uncorrected information for the purpose of notifying them of the amendment.

Procedures for Amendment of Internal Records

When a patient's request for amendment of protected health information is approved, either the records containing the affected information will be updated or the amended information will be linked to the information.

Procedures

- The Privacy Official will refer the request for amendment to the staff member responsible for maintaining the affected records
- That staff member will identify the records that need to be amended
- Those records should either be amended or should be linked to the amended information (that is, contained in a new or corrected record where it will be available when the affected information is used or disclosed in the future)

The Privacy Official will receive complaints regarding amendments to health information.

Notification of Recipients of Amended Information

When a patient's protected health information is amended in response to a request received from the patient, other organizations to which the information being amended has been disclosed will be notified of the amendment.

Organizations to be notified include:

- Business associates, health plans, and other providers that the Privacy Official can identify as having received the information
- Persons and organizations the patient can identify as having received the information that requires amendment, but only to the extent that the Privacy Official can confirm that these persons or organizations received the information

It is not necessary to confirm that the organizations or other entities notified of the amendment have taken any action to update their own records.

Denial of Request for Amendment

When a request to amend protected health information is denied, the patient will be informed in writing of the decision. The notice sent to the patient must be written in plain language and advise the patient of the following:

- Reason for denial
- He or she may submit a statement of disagreement that will become part of his or her records and will, in the future, be disclosed to any person or organization that receives the identified information
- He or she may ask the provider to include the request for amendment and the denial in any future disclosure of the identified information to any person or organization

that receives the identified information
- He or she may file a complaint with the provider concerning the request for amendment (a description of how the patient can file this complaint must be included in the notice)

The letter must identify the name, mailing address, and telephone number of the Privacy Official.

Statement of Disagreement

If the patient submits a statement of disagreement when notified that a request for Amendment of protected information has been denied, the Privacy Official will review it and will append it to or otherwise link it to the patient's record. This will ensure that it will accompany the original information when it is used or disclosed in the future.

The Privacy Official may prepare an accurate summary of the patient's statement of disagreement if he believes that it will adequately provide a clear understanding of the disputed information.

Rebuttal of Disagreement

If a patient submits a statement of disagreement when notified that his or her request for amendment of protected health information has been denied, the Privacy Official will review the statement and determine whether a formal rebuttal or response, as provided for in federal regulations, is necessary. If it is determined that a rebuttal is necessary, he or she will prepare and append it to the patient's records.

Procedure

- The Privacy Official will consult as necessary with the patient's physician, health care professional or other staff to make this determination
- Both the patient's statement of disagreement and the rebuttal statement will be noted in the patient's records
- The statement of disagreement and the rebuttal either will be included in the patient's records, or will be linked to those records to permit them to be included with the original information when it is used or disclosed in the future
- A copy of the rebuttal statement will be sent to the patient

Receipt of Notification of Amendment

When a notification of amendment of protected health information is received from a medical practice, health plan, or other covered entity, it will be handled as though it were an amendment approved by the University.

Storage and Maintenance

Storage and Maintenance of Patient Information

Each unit and department which creates, maintains or handles protected health information will establish and maintain policies and procedures on the storage and maintenance of patient information.

The University will maintain records for a minimum of six years.

The Compliance Officer will insure that only appropriate staff members, including work-study and graduate students when appropriate, have access to the records.

All storage and maintenance policies and procedures will be approved by the Privacy Official.

Accounting

Accounting for Disclosures

The University will establish and maintain procedures for developing the Notice of Privacy Practices form and obtaining patient authorization for use and disclosure of protected health information for purposes other than treatment, payment or healthcare operations.

Maintenance of Records of Disclosures

The Privacy Official will create a system for documenting all disclosures of protected health information for which an individual may request an accounting.

Disclosures of protected health information that the University is not required to report to a patient include:

- Any disclosure for the purpose of treatment, payment, or the day-to-day operation of the University
- Any disclosure to the patient personally
- Any disclosure for use in a facility directory
- Disclosures that are part of a limited data set
- Disclosures that are incidental to another permissible use or disclosure
- Disclosures authorized by the patient
- Any disclosure to national security or intelligence agencies that is required by law
- Any disclosure to correctional institutions or law enforcement agencies that is required by law

- Any disclosure that occurred prior to April 14, 2003, the effective date of the HIPAA privacy rules

Disclosure Accounting to Patients

Procedure to Request an Accounting of Disclosures

To receive an accounting of disclosures of protected health information, a patient must submit a written request to the administrator of the department or unit.

Accountings must include disclosures made during the 6 years prior to the request, including disclosures to, or by business associates.

Procedure

- A patient who indicates to any staff member that he or she would like to receive an accounting of disclosures should be told to contact the administrator
- The administrator will provide the patient with a disclosure accounting form and review the types of disclosures that will be reported in the accounting
- The administrator will determine whether a law enforcement or health oversight agency has requested a suspension of the patient's right to receive an accounting of disclosures
- If the patient's right to an accounting has not been suspended, the administrator will initiate the preparation of an accounting

Charges for Accountings of Disclosures

If an individual requests more than one accounting during any 12-month period:

- The individual will not be charged for the first requested accounting in a 12-month period
- If an individual has received an accounting for which he or she was not charged during the preceding 12 months, he or she will be informed that the University will charge a reasonable fee for the accounting. If the patient agrees to pay this fee, the accounting will be provided

Suspension of a Patient's Right to Receive an Accounting of Disclosures

A law enforcement or health oversight agency may request the provider to suspend the right of an individual to request an accounting of disclosures.

Requests from law enforcement agencies should be submitted in writing. The written statement should indicate that providing an accounting is likely to impede the agency's activities and should specify a time period during which the patient's right will be suspended.

A request that is received verbally must be confirmed in writing. If a written request is not submitted, the individual's right to an accounting may be suspended for no more than 30 days.

Procedures

- A communication from a law enforcement or health oversight agency requesting the suspension of a patient's right to an accounting of disclosures should be directed to the Privacy Official
- The Privacy Official will verify the credentials of the government official that makes a verbal request and document the identity of the official or agency
- The Privacy Official will place the patient's name on a list of persons whose right to an accounting has been suspended pursuant to an official request

Information To Be Provided in an Accounting of Disclosures

The information that will be provided in an accounting of disclosures includes:

- The date of the disclosure
- The name of the entity or person who received the protected health information
- A brief description of the purpose of the disclosure or a copy of the authorization for the disclosure

Documentation of Accountings Provided to Patients

A copy of any accounting provided to a patient will be retained for a period of six years from the date the accounting is provided.

Documentation of Disclosures Requiring an Accounting

All disclosures of protected health information that must be included in an accounting of disclosures will be documented by the staff making the disclosure.

Procedure

- Any disclosure, other than those listed in this section not required to be included in the accounting, will be documented by completing a disclosure accounting form
- The disclosure accounting form will be forwarded to the Privacy Official, who will update the files and databases from which the accounting of disclosures was prepared

Complaints and Breaches

The University will maintain and establish policies and procedures for dealing with and the resolution of complaints and breaches.

Resolution of Complaints and Breaches

The Privacy Official will implement the procedures established by which a patient or other individual may file a complaint concerning the privacy policies and procedures that have been adopted by the University, or the compliance of staff with those policies.

The Privacy Official also will implement the procedures established to mitigate the harmful effect of uses or disclosures of protected health information that violate the privacy policies and procedures established by this manual.

Submission of complaints

A patient or other individual who wants to file a complaint concerning privacy practices, including privacy policies and procedures, or concerning a suspected disclosure of protected health information that violates federal or state law or the privacy practices of the University or any other unit or department of the University should use the following procedure:

- If the patient asks how to file a complaint, he or she should be informed that he or she may contact the Privacy Official and be provided with the telephone and mailing address of the individual. The patient should also be informed on how to file a complaint directly with the Secretary of the U.S. Department of HHS
- The Privacy Official will provide the patient with a copy of the complaint form and direct the patient to complete the form and either mail it to the address printed on the form or leave the form with the administrator of the office or agency

These procedures are summarized in the Notice of Privacy Practices as follows: If you would like to submit a comment or complaint about privacy practices, you can do so by contacting the administrator and requesting a privacy practices complaint form or by sending a letter outlining your concerns to the University Privacy Official.

If you believe that your privacy rights have been violated, you should call the matter to our attention by sending a letter describing the cause of your concern to the same address.

You will not be penalized or otherwise retaliated against for filing a complaint.

Complaint Resolution Procedures

The Privacy Official will implement the procedures which address resolution of complaints concerning privacy policies and procedures and which addresses resolution of complaints involving the violation of privacy policies and procedures.

Complaints Concerning Privacy Policies and Procedures

The procedures for resolution of complaints submitted by patients or other individuals concerning the privacy practices of the University or the policies and practices established in this manual are outlined below.

- Upon receiving a complaint the Privacy Official or a designated staff member will review the complaint, evaluate the specific details of the complaint, and determine whether the complaint warrants a change in the University's privacy policies or procedures
- If a change appears to be warranted, the staff member conducting the evaluation will develop a recommendation and submit it to the Privacy Official, who will determine whether an immediate change in policies and procedures is needed to prevent a violation of federal or state privacy standards, laws or regulations
- If the University determines that a change in policies and procedures is necessary, a revised policy will be prepared following the procedures outlined in this manual. A response should be prepared for signature by the Privacy Official and sent to the individual submitting the complaint. The response should thank the individual for his or her interest. It should indicate that the suggestion has been evaluated, and while the University believes that its current practices comply with federal and state requirements, it is considering changes in privacy practices, policies, and procedures to address the patient's concerns
- If a change does not appear to be warranted, a response to the complaint will be prepared for signature by the Privacy Official, and sent to the individual submitting the complaint. The response should thank the individual for his or her interest. It should indicate that the suggestion has been evaluated, but that the University believes that its current practices comply with federal and state requirements and are sufficient to protect the individual's privacy
- Receipt of the complaint and its final disposition should be documented using the procedures established in this manual

Complaints Arising from Possible Violation of Privacy Policies

The procedures for resolution of complaints submitted by patients or other individuals concerning the disclosure of protected health information are outlined below.

- A staff member who receives a complaint from a patient or other individual that concerns a possible use or disclosure of protected health information that violates the University's privacy policies and procedures or that violates federal and state law should immediately refer the complaint to the Privacy Official
- The Privacy Official will review the complaint and determine whether a violation occurred, and if so, whether the violation involves only the privacy policies and practices established in this manual, or also involves a violation of federal and state privacy laws and standards
- If the Privacy Official determines the complaint may involve a violation of federal or state standards and legal requirements, he or she will immediately forward the complaint to the University's legal counsel for evaluation. The request for evaluation should specify a date by which the evaluation should be completed. The Privacy Official

should follow-up and track the status of the referral. If the evaluation indicates that federal or state standards may have been violated, the mitigation procedures established in this manual should be followed
- If the Privacy Official determines that the complaint does not involve a violation of federal or state standards and legal requirements, he or she will determine whether the University's privacy policies and procedures were violated. If policies and procedures have been violated, the disciplinary procedures established in this manual should be initiated
- Upon completion of the previous step the Privacy Official should contact the person submitting the complaint and notify him or her of the actions that will be taken to address the complaint
- Evaluations of complaints should generally be completed within 30 days of receipt
- The receipt of the complaint and the final disposition should be documented

Documentation of Complaints

The Privacy Official will establish and maintain files containing documentation of all complaints received. This documentation will include the actions taken to address or resolve the complaint, including any written correspondence with the person submitting the complaint.

Mitigation

When the Privacy Official determines that a use or disclosure of protected health information has violated the policies and procedures established by this manual, the case will be referred to the University's legal counsel to:

- Determine any action needed to mitigate any harm that may result to the patient whose information was used or disclosed
- Evaluate the University's legal exposure and recommend a course of action
- Follow-up with the individual

All communications with the complaining individual concerning use or disclosure of protected health information that legal counsel determines may violate federal or state standards and legal requirements should be handled by the University's legal counsel.

Education, and Training

The University will maintain policies and procedures related to privacy and security awareness, education and training.

Training will be developed and implemented in a manner that will raise employees' awareness of threats to the privacy and security of patient information.

Training will outline the actions that are required in order to minimize these threats.

Specific objectives for staff participating in privacy security awareness and training include:

- Increased awareness of the need to protect systems resources
- Understanding of the University's security policies and procedures
- Understanding of the security skills needed to effectively use the University's information resources

Specific topics that must be covered in security training include:

- Workstation configuration and use
- Management of user IDs and passwords
- Avoidance, detection, and removal of computer viruses
- Contingency plans and procedures for continued operation during emergencies or system failures
- Introduction of the Security Officer and his/her responsibilities
- Steps to take when a potential security violation is detected

Security

Work Environment Security

The University will establish and maintain policies and procedures designed to prevent unintentional or inadvertent disclosure or release of information in or around employee's work areas and environment.

Physical Configuration of Work Areas

All work areas where protected health information is created or used must be designed so that equipment can be positioned to prevent unauthorized persons, including patients and vendors, from viewing patient information that may be displayed on a workstation monitor.

Workstation Configuration

All workstations where protected health information is created or used (i.e., computers connected to the University's network) must require users to log on before accessing patient information. Workstations must display a warning that reminds users of the University's security requirements before permitting them to access patient information.

Workstation Usage

All staff members must comply with the following requirements to protect the security of information accessed from a workstation where protected health information is available:

- Do not permit another staff person to use his or her workstation without first logging off and having the other staff person log on using his or her own user ID and password unless the process of logging off and on would endanger the health or safety of a patient, and only when the other staff person is known to be authorized to access patient records
- Log off of his or her workstation whenever it will be left unattended for any length of time
- Shut down his or her workstation at the end of the business day
- Enable (or not disable) virus scanning software and promptly report any virus alerts to the Security Official
- Install and use only software that has been approved by the Security Official
- Do not share password with co-workers, or friends and family who visit the practice

Contingency Pans

The University will establish and maintain policies and procedures for contingency plans that include applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures

Scope and Purpose of Contingency Plans

The University’s contingency plan establishes procedures for responding to natural disasters, vandalism (including computer viruses), system failures, power failures, or other events that would disrupt normal operation of the practice's information systems. The purposes of the contingency plan are:

- To prevent unauthorized access to patient information when normal controls over access may be disrupted
- To maintain uninterrupted availability of critical information while the practice continues to operate and provide patient care
- To prevent disruptions of normal operations that could result in the loss, destruction, or corruption of information maintained electronically

Responsibility for Contingency Planning

The Security Official is responsible for developing, approving, disseminating, and implementing the contingency plan. He or she is specifically responsible for:

- Developing, testing, and updating contingency plans for all aspects of information systems operation
- Ensuring the delegation of appropriate authority and training of personnel responsible for implementing elements of the contingency plan, including regular back-up of critical data
- Ensuring the availability of appropriate staff to implement contingency plans during normal hours of operation, i.e., when information systems support is needed by the staff
- Providing appropriate information and training for all staff on contingency plans and operating procedures to be used during emergencies

Identification of Critical Systems and Data

The Security Official will prepare and regularly update a contingency plan that identifies the following:

- Critical applications that are vulnerable to disruption during an emergency
- Critical information that may be lost during an emergency

Critical applications include, but may not be limited to, those that create, manipulate, store, retrieve, or transmit personal health information.

An application is vulnerable if its disruption during an emergency might cause the loss or destruction of critical information or allow an unauthorized person to access the information. Critical information includes at least the patients' health information.

Alternate Arrangements for Critical Applications

For all critical applications and information the Security Official will establish:

- A time period that represents the maximum delay during which the processing performed by an application can be deferred, or during which critical information may be unavailable
- An alternate means of running critical applications and ensuring the availability of critical information alternative means of running critical applications and accessing critical information may include the maintenance of back-up systems or arrangements to transfer processing to an alternative site or vendor

The Security Official must obtain reasonable assurances that alternate sites or back-up systems would be available in the event of a disaster. The ability of alternative arrangements to support critical applications and enable access to critical information must be documented during tests of the contingency plan.

Hardware Backup Plans

The contingency plan must include provisions for the transfer of processing to alternative or back-up hardware in the event of the failure of a piece of equipment. All back-up equipment must be compatible with and capable of performing all functions that are performed by the primary equipment. Back-up equipment is not required to be available on-site, but must be available for installation within the timeframes established for outages of critical systems.

Back-up Procedures

The contingency plan must establish procedures for the regular backup of all critical applications and information.

Back-up of Critical Applications

The Security Official must ensure that any critical applications can be promptly restored if damaged as the result of a hardware failure or other operating contingency.

Staff responsible for the operation of the University's information systems must be able to re-install and re-initialize all critical software within a period of time that is specified in the contingency plan.

The contingency plan must also contain procedures for activating alternative arrangements to support the affected functions when efforts to re-establish the operation of critical applications do not succeed within the specified time period.

Back-up of Critical Information

All critical information will be backed up on a regular schedule to prevent the permanent loss of information due to system failure or natural disaster.

Recovery Procedures

The contingency plan must establish procedures for restoring applications and information affected by a system failure.

The recovery effort would be considered complete when the University's information systems have been restored and are capable of performing their normal functions, and any backlog created by the system failure has been cleared.

IT Personnel Availability

Staff members responsible for the operation of the University's information systems must be available at all times during normal business hours. While it is not required that they physically be present at the University's facilities which create or handle personal health information, they must be accessible by telephone for consultation, and must be available to diagnose system failures and implement corrective actions at all times.

Operating Procedures

The contingency plan must establish operating procedures for safeguarding the security of information that is affected by any system failure or any disruption of normal operations. These procedures must prevent unauthorized users from gaining access to patient information when normal operating safeguards are not functioning.

The plan also must include a method of communicating the status of efforts to restore normal functions to users who are affected by a system failure or disaster.

Testing the Contingency Plan

All elements of the contingency plan must be tested to determine that they will, in fact, provide necessary functionality and protect the security of patient information.

Each component of the contingency plan should be tested individually. Examples of individual components include procedures for transferring processing from the primary equipment to back-up equipment, procedures for backing up and restoring critical information, and procedures for transferring processing to an alternative site.

These tests of the contingency plan are vital to ensure the smooth implementation of procedures for responding to emergencies and to assure continued support for critical functions. Staff members with specific responsibilities in the recovery operation must be given an opportunity to practice their roles in a realistic test situation.

Once the individual components have been tested, a final test of the contingency plan should be conducted to simulate the response to a complete systems failure. The results of the final test should be evaluated by the Security Officer and the staff responsible for the operation of the information systems. The contingency plan should be revised as appropriate, in response to the test.

The contingency plan should be tested at least once each year.

Implementation Procedures

The contingency plan must list the specific procedures to be taken for implementing it in the event of a disaster or other disruption of normal operations.

These should include procedures staff members should follow to report possible system failures and to obtain information on the current status of the practice's information systems.

All users must be familiar with the contingency plan procedures and must thoroughly be briefed on pertinent aspects of the plan.

Information Technology Security Measures

The policies in this section address security protections that are dependent on the information technology (hardware and software) the University uses to manage patient information.

Physical Security of Hardware and Software

The Security Official will establish procedures to:

- Ensure the physical security of all hardware, software, and information stored and processed in the practice

- Ensure physical access control for information systems technology used by the practice (e.g., file servers, databases, etc.)

Installation, Maintenance, and Removal of Hardware

The Security Official will maintain a complete inventory of all information systems hardware owned or leased by the University.

He or she will establish procedures that provide for:

- Issuing property or inventory-control numbers for all equipment
- Documenting all software installed on information systems equipment used in the medical practice
- Creating maintenance records for all equipment, including reports of malfunctions and records of any modification or replacement of components
- Removing information that must be kept secure when equipment is sent out of the facility for maintenance
- Destroying information contained on information systems equipment prior to disposal
- Documenting information systems equipment that leaves the University's premises

Handling Information-Storage Media

The Security Official will maintain a complete inventory of all information storage media that hold patient and other information.

He or she will establish procedures that provide for:

- Secure storage of all data storage media
- Restriction of handling of data storage media to qualified staff members
- Documentation of any removal or return of storage media to or from the secure areas in which they are stored
- Documentation of all back-up data tapes or media

Procedures for Data Destruction

The Security Official will establish procedures that must be followed when data storage media are being replaced or destroyed.

These procedures must provide for verifying that patient information has effectively been removed from the storage media and cannot be recovered from the storage media. For example, when a fixed disk drive that has been used to store patient information is disposed of, not only must the data be deleted from the drive, but the drive itself also must be reformatted or otherwise treated to ensure the complete destruction of any information that it may have contained.

Passwords

All users must establish and maintain passwords that comply with the following policies:

Password Selection

A user password must:

- Contain a minimum of six alpha numeric characters
- Not contain the user's user ID, name (or portion of), birth date, social security number (or portion of), family members name, nick name anniversary, hobby, telephone number (or portion of) or any information that can be easily guessed because the user refers to it routinely yet not be so complicated that it has to be written down

Information systems staff are responsible for implementing technical measures such as automatic password validation to enforce this policy.

Updating and Maintenance of Passwords

A user must change his or her password every 90 days.

A user will receive a reminder to update his or her password at least five days prior to the password's expiration date. This warning will be repeated every day when the user logs onto the system.

Information systems staff are responsible for implementing technical measures to enforce this policy.

Procedures for Validating Passwords

Information systems that are protected by passwords must lock out a user's account if more than three incorrect attempts are made to log on.

A user who is locked out must contact the staff member responsible for operating the information system and request a new password.

Issuance of New Passwords

A user who has forgotten his or her password, who believes that his or her password has been made known to another user, or who has been locked out of the information system should contact the staff member who is responsible for administration of user passwords.

The password administrator will confirm the identity of the user and then reset the password in a manner that requires the user to select a new password the next time he or she logs on.

The password administrator will review an employee's need for a new password and or increased access whenever the employee's job function changes.

The password administrator will block all access once an individual is terminated, preventing them their access to protected information.

Communications and Network Security

Information Technology will develop and maintain policies that address measures the University must take to ensure the security of information that either is transmitted over a communications network or can be remotely accessed by users of its information systems.

Incident Reporting and Investigation

The policies and procedures in this section of the security manual are designed to detect, and resolve in a timely manner, adverse events that may result in:

- Unauthorized access to information systems and patient information
- Unauthorized alteration, damage, or destruction of information
- Unauthorized release of data
- Disruption of information system operation that may impair access to patient information

Responsibility for Incident Investigation

The Security Official will:

- Ensure the implementation of mechanisms to detect unauthorized access of information systems and resources, including patient information
- Maintain a log of all reports of security-related incidents or violations of security policies policies and procedures review all reports of security incidents and evaluate their severity identify corrective actions to prevent future incidents
- Oversee the implementation of corrective actions

Incident Reporting

All staff members and contractors who use the University's information systems must report actual or suspected security intrusions, incidents or violations to the Security Official.

Procedure

- A staff member should notify his or her immediate supervisor or manager of all suspected security incidents
- The supervisor should evaluate the suspected incident and determine whether it involves a breach of security policies or procedures
- If a breach has occurred, the incident should be promptly reported to Security Official

Auditing

The Security Official will implement technologies and procedures that will enable a security audit to:

- Identify when users were logged onto the system
- Identify the information they accessed when they were logged on
- Reconstruct the circumstances leading up to the disruption of normal operations, determine when the disruption occurred, and describe the nature of the disruption
- Identify unauthorized access and document when the unauthorized access occurred or was attempted)
- Identify the information that was accessed without authorization

The Security Official will periodically review audit logs to identify changes that may be required in security policies and procedures.

Specific audits will focus on:

- The disruption of normal operations to determine whether contingency plans were successful in preserving the security of information and preventing unauthorized access
- Unauthorized access, to determine whether security was breached and what actions may be needed to strengthen defenses against unauthorized access

APPENDIX 1

Compliance Officials:

Cindy Vetter
Director
University of Northern Colorado
Campus Box 2
Greeley, CO 80639
970-351-2711

Dan Satriana
General Counsel
University of Northern Colorado
Campus Box 29, Carter Hall, Room 4003
Greeley, CO 80639
970-351-2399

Privacy Officials:

Same as Compliance Officials

Security Official:

Matt Langford
Director, Information Technology
University of Northern Colorado
Campus Box 19, Carter Hall, Room 14
Greeley, CO 80639
970-351-1420

APPENDIX 2
HIPAA FORMS

UNIVERSITY OF NORTHERN COLORADO
CONFIDENTIALITY AND INFORMATION SECURITY AGREEMENT

Staff, faculty, students and all other individuals (vendors, temporary employees, etc.) under the control of the University of Northern Colorado ("UNC") (department of organization) are required to maintain the confidentiality of patient, clinical, financial, or other sensitive information. UNC employees will be held personally responsible for safeguarding security log-in processes, passwords and electronic signatures. UNC employees must strictly adhere to standards that govern authorized access to, use and/or disclosure of sensitive and confidential information. Failure to do so may result in disciplinary action, up to and including termination of employment. You are required to sign this document as a condition of employment.

I ACKNOWLEDGE, UNDERSTAND, AND AGREE:

1. The types and categories of written, verbal, electronic or printed are considered to be confidential ("CONFIDENTIAL INFORMATION") includes, but is not limited to: (a) medical records; (b) clinic medical records; (c) physician's private patient records; (d) medical records received from other health care providers; (e) correspondence addressed to or from employees of UNC concerning a specific, identifiable patient; (f) patient information verbally given to me by the patient or other persons; (g) diagnoses; (h) assessments; (i) medical histories; (j) operative reports; (k) discharge summaries; (l) nursing notes; (m) medications; (n) treatment plans; (o) follow-up care plans; (p) requests for and results of consultations; (q) results of laboratory, or other medical tests; (r) demographic data; (s) financial/-funding information; and (t) all other types and categories of information to which I know or have reason to know the UNC intends or expects confidentiality to be maintained.

2. Services provided by the UNC for its patients/students and all documents and information related to such services are private and CONFIDENTIAL INFORMATION.

3 . Patients/students furnish information to the UNC with the understanding and expectation that it will be kept confidential and used only by authorized persons, within the scope of his/her employment, as necessary, to provide needed services.

4. CONFIDENTIAL INFORMATION stored in electronic form must be treated with the same medical/legal care as data in the paper chart.

5. My access to CONFIDENTIAL INFORMATION subjects me to legal guidelines and obligations.

6. I will comply with all information security policies and procedures in effect at UNC.

7. I will access data only in accordance with policies and standards.

8. My security code (logon, password and electronic signature) is equivalent to my legal signature. I will be personally accountable for all access or use performed under these codes.

9. By reason of my duties or in the course of my employment I may receive or have access to verbal, written or electronic information concerning patients/students, staff and services performed by the UNC. I will not inappropriately access, use, or disclose (verbally, in written form, or by electronic means) to any person, or permit any person to inappropriately access; use, or disclose any reports or other documents prepared by me, coming into my possession or control, or to which I have access, nor any other information concerning the patients, staff or operations of the UNC at any time, during or after my employment.

10. If and when my employment or assignment with the UNC ends, I will not inappropriately access, use, disclose, retain, or copy any reports or other documents prepared by me, coming into my possession or control, or to which I have access, nor any other information concerning the patients/students, staff or operations of the UNC.

11. I will not destroy or erase any data or information in any form located in or stored in UNC computers or files unless it is part of routine computer maintenance.

12. I will use discretion to assure conversations that include CONFIDENTIAL INFORMATION cannot be overheard by persons who do not have a "need to know" when information must be discussed with others in the performance of my duties.

13. I will adhere to UNC procedures governing proper handling or disposal of printed material containing individually identifiable information.

14. I will notify my supervisor and the UNC Privacy Officer immediately, but not later than one business day, of any actual or suspected inappropriate use, access, or disclosure of CONFIDENTIAL INFORMAITON, whether by me or anyone else, whether intentional or accidental. There will be NO retaliation for filing a legitimate complaint.

15. I will maintain the confidentiality of all information concerning patients, staff, or operations of UNC regardless of the method of retrieval, including information obtained on home-based or off-site personal computers.

16. The inappropriate access, use, or disclosure of information by me may violate state and/or federal laws and may subject me to civil damages and criminal prosecution, and to disciplinary action, up to and including termination.

17. All documents, encoded media, and other tangible items provided to me by UNC or prepared, generated, or created by me in connection with any activity of UNC are the property of the UNC.

18. The UNC as the holder of data, reserve the right to, and may monitor and audit, all information systems for security purposes.

19. Security codes (logon, password and electronic signature) are the user's way to verify his/her identity and should be difficult for someone else to guess. Use of names, birth dates phone numbers, etc. is not allowed. I will choose security codes carefully and not disclose them to anyone.

20. I will not disclose security codes to anyone nor will I attempt to learn another person's security codes. Any misuse of my confidential security code will be a violation of UNC policy and will subject me to disciplinary action, up to and including termination.

21. Security codes must not be written on paper that is accessible to anyone but the user and must not be visible around the terminal/workstation.

22. I may access my own health information via an electronic application, pursuant to established policies, but I may not access that of my spouse, children, family members, or co-workers unless I am involved in their direct care.

23. I will not access data on patients/students or other individuals for whom I have no responsibility or for whom I have no "need to know." Audit trails will track unauthorized access.

24. I will immediately contact Information Technology (IT)to obtain a new security code if I have reason to believe the confidentiality of my security code has been breached.

25. Regardless of the site of access, information must be treated as confidential. Unauthorized access or release of confidential information will subject me to disciplinary action, up to and including termination.

26. I will take reasonable steps, such as using a screen saver with a password, to keep my workstations and logins as secure as possible to minimize the risk of unauthorized use of either.

27. I will refrain from making unauthorized copies of data or applications. Loading of viruses, unauthorized queries, and other interference with computer resources will subject me to disciplinary action, up to and including termination.

28. If I receive access to information stores such, as the IT's data warehouse, or other databases containing CONFIDENTIAL INFORMATION, I will use that access only for the intended and stated purpose and will

not provide access to 3rd parties without the explicit written permission of the IT's data steward. I will utilize data obtained from such information stores in conjunction with data use policies.

29. This signed document will become a part of my permanent personnel record.

Information Technology Services personnel will never ask for your password. If someone does ask for my password, I will report it immediately to the Security Official identified in the HIPAA Policy and Procedures Manual.

BY SIGNING THIS AGREEMENT, I ACKNOWLEDGE AND REPRESENT that
I have read and understand the foregoing UNC Confidentiality and Information Security Agreement.

Employee Information

Name _____
(Please Print)

Telephone #
and Pager _____

Position
and Title _____

Assigned Unit/-
Department _____ _____

Today's
Date _____

Employee
Signature _____

UNIVERSITY OF NORTHERN COLORADO

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The Health Insurance Portability & Accountability Act of 1996 (HIPPA) requires all health care records and other individually identifiable health information (PROTECTED HEALTH INFORMATION) used or disclosed to us in any form, whether electronically, on paper, or orally, be kept confidential. This federal law gives you, the patient, significant new rights to understand and control how your health information is used. HIPAA provides penalties for covered entities that misuse personal health information. As required by HIPAA, we have prepared this explanation of how we are required to maintain the privacy of your health information and how we may use and disclose your health information.

Without specific written authorization, we are permitted to use and disclose your health care records for the purposes of treatment, payment and health care operations.

- **Treatment** means providing, coordinating, or managing health care and related services by one or more health care providers.
- **Payment** means such activities as obtaining reimbursement for services, confirming coverage, billing or collection activities, and utilization review.
- **Health Care Operations** include the business aspects of running our clinics, such as conducting quality assessment and improvement activities, auditing functions, cost-management analysis, and customer service. An example would include a periodic assessment of our documentation protocols.

In addition, your confidential information may be used to remind you of an appointment (by phone or mail) or provide you with information about treatment options or other health-related services including release of information to friends and family members who are directly involved in your care or who assist in taking care of you. We will use and disclose your PROTECTED HEALTH INFORMATION when we are required to do so by federal, state or local law. We may disclose your PROTECTED HEALTH INFORMATION to public health authorities who are authorized by law to collect information, to a health oversight agency for activities authorized by law included but not limited to: response to a court or administrative order, if you are involved in a lawsuit or similar proceeding, response to a discovery request, subpoena, or other lawful process by another party involved in the dispute, but only if we have made an effort to inform you of the request or to obtain an order protecting the information the party has requested. We will release your PROTECTED HEALTH INFORMATION if requested by a law enforcement official for any circumstance required by law. We may release your PROTECTED HEALTH INFORMATION to a medical examiner or coroner to identify a deceased individual or to identify the cause of death. If necessary, we also may release information in order for funeral directors to perform their jobs. We may release your PROTECTED HEALTH INFORMATION to organizations that handle organ, eye or tissue procurement or transplantations, including organ donations banks, as necessary to facilitate organ or tissue donation and transplantation if you are an organ donor. We may use and disclose your PROTECTED HEALTH INFORMATION when necessary to reduce or prevent a serious threat to your health and safety or the health and safety of another individual or the public. Under these circumstances, we will only make disclosures to a person or organization able to help prevent the threat. We may disclose you PROTECTED HELTH INFORMATION if you are a member of U.S. or foreign military forces (including veterans) and if required by the appropriate authorities. We may disclose your PROTECTED HEALTH

INFORMATION to federal officials for intelligence and national security officials in order to protect the President, other officials or foreign heads of state, or to conduct investigations. We may disclose your PROTECTED HALTH INFOMAION to correctional institutions or law enforcement officials if you are an inmate or under the custody of a law enforcement official. Disclosure for these purposes would be necessary: (a) for the institution to provide health care services to you, (b) for the safety and security of the institution, and/or (c) to protect your health and safety or the health and safety of other individuals or the public. We may release your PROTECTED HEALTH INFORMATION for workers' compensation and similar programs.

Any other uses and disclosures will be made only with your written authorization. You may revoke such authorization in writing and we are required to honor and abide by that written request, except to the extent that we have already taken actions relying on you authorization.

You have certain rights in regard to your PROTECTED HEALTH INFORMATION, which you can exercise by presenting a written request to our Privacy Official at the address listed below:

- The right to request restrictions on certain uses and disclosures of PROTECTED HEALTH INFORMATION, including those related to disclosures to family members, other relatives, close personal friends, or any other person identified by you. We are, however, not required to agree to a requested restriction. If we do agree to a restriction, we must abide by it unless you agree in writing to remove it.

- The right to request to receive confidential communications of PROTECTED HEALTH INFORMATION from us by alternative means or at alternative locations.

- The right to access, inspect and copy your PROTECTED HEALTH INFORMATION.

- The right to request an amendment to your PROTECTED HEALTH INFORMATION.

- The right to receive an accounting of disclosures or PROTECTED HEALTH INFORMATION outside of treatment, payment and health care operations.

- The right to obtain a paper copy of this notice from us upon request.

We are required by law to maintain the privacy of your PROTECTED HEALTH INFORMATION and to provide you with notice of our legal duties and privacy practices with respect to PROTECTED HEALTH INFORMATION.

We are required to abide by the terms of the Notice of Privacy Practices currently in effect. We reserve the right to change the terms of our Notice of Privacy Practices and to make the new notice provisions effective for all PROTECTED HEALTH INFORMATION that we maintain. Revisions to our Notice of Privacy Practices will be posted on the effective date and you may request a written copy of the Revised Notice from this office.

You have the right to file a formal, written complaint with us at the address below, or with the Department of Health and Human Services, Office of Civil Rights, in the event you feel your privacy rights have been violated. We will not retaliate against you for filing a complaint.

For more information about our Privacy Practices, please contact:

The University Counsel
University of Northern Colorado
Carter Hall, Room 4003
Greeley, CO 80639
970-351-2399

For more information about HIPAA or to file a complaint:

The U.S. Department of Health & Human Services
Office of Civil Rights
200 Independence Avenue, S.W.
Washington, D.C. 20201
877-696-6775 (toll-free)

Patient Information Amendment Form

I, _____ (Patient's name) request that information kept in the records of the University of Northern Colorado be amended.

Information to be Amended

The following information needs to be amended:

Item to be changed:

Data source:

Change:

Reason:

If you need help with this form, please contact:

University of Northern Colorado Privacy Official
Telephone Number: 970-351-2399

Attach additional copies of this page as needed.

_____ _____
Signature of Patient of Personal Representative: Date

_____ _____
Print Name of Patient or Personal Representative

Description of Personal Representative's authority and attach document evidencing authority, such as a Power of Attorney

This section to be filled out by Privacy Official
Approved Amendments

The following requests for amendment of information have been

Θ Approved. The information will be corrected and other organizations to which this information has been disclosed will be notified as required by federal regulations.

Θ Denied. The request was denied for the following reasons:

Patient Request for Confidential Communication

I, _____ hereby request confidential communication of protected health information.

Designated Method of Contacting the Patient

Communications with the patient named above should be directed to:

Mailing Name

Street Address

City, State & Zip

Telephone Number

Name of Patient: _____

Address of Patient: _____

_____

_____ _____

Signature of Patient or Personal Representative: **Date**

_____ _____

Print Name of Patient or Personal Representative

Description of Personal Representative's authority and attach document evidencing authority, such as a Power of Attorney

Acknowledgment of Receipt of Privacy Practices

I, _____ have received a copy of the University of Northern Colorado Notice of Privacy Practices with an effective date of _____

Name of Patient: _____

Address of Patient: _____

_____

_____ _____
Signature of Patient or Personal Representative: Date

_____ _____
Print Name of Patient or Personal Representative **Description of Personal Representative's authority and attach document evidencing authority, such as a Power of Attorney**

Name of Witness

Signature of Witness _____ Date _____

Authorization Revocation Form

This notion revokes the authorization to the use and disclosure of protected health Information for: _____ that was signed on _____

Effect of Revocation

Protected health information that is collected on or after the date on which this form is received by the University of Northern Colorado will not be used or disclosed by the University of Northern Colorado for the purposes specified in the authorization that is revoked. This revocation of authorization will not limit the ability of the University of Northern Colorado to seek payment for services that it provided under an earlier authorization, nor to meet legal obligations related to those services, nor will it affect uses or disclosures under the revoked authorization that occurred prior to the effective date of this revocation.

Other consequences of revoking authorization include:

This revocation of authorization to use or disclose protected health information is effective on _____.

Name of Patient _____

Address of Patient _____

_____

_____ _____
Signature of Patient or Personal Representative: Date

_____ _____

Print Name of Patient or Personal Representative	**Description of Personal Representative's authority and attach document evidencing authority, such as a Power of Attorney**

Authorization for Use or Disclosure of Protected Health Information

I, _____ authorize the University of Northern Colorado, their administrative and clinical staff to (check all that apply):

- Θ use the following protected health information, and/or
- Θ disclose the following protected health information to:

Information to be used or disclosed.

This protected health information is being used or disclosed for the following purposes:

1.

2.

3.

Θ The patient has requested this information be used and disclosed but does not wish to specify the purpose.

This authorization shall be in force and effect until _____(date) at which time this authorization to use or disclose this protected health information expires.

I understand that I have the right to revoke this authorization, in writing, at any time by sending such written notification to:

Privacy Official of University Counsel
Campus Box 29
4003 Carter Hall
University of Northern Colorado
Greeley, CO 80639

I understand that a revocation is not effective to the extent that my health care provider has relied on the sue or disclosure of the protected health information or if my authorization was obtained as a condition of obtaining insurance coverage and the insurer has a legal right to contest a claim or if my authorization was required for treatment provided by participating in a research study.

I understand that information used or disclosed pursuant to this authorization may be disclosed by the recipient and may no longer be protected by federal or state law.

I understand that if I refuse to sign this authorization I may not be eligible for, or receive research-related treatment or treatment that I have requested for the purpose of disclosure
to others.

Θ The use or disclosure requested under this authorization will result in direct or indirect remuneration to the University of Northern Colorado from a third party.

Θ The use or disclosure requested under this authorization will **not** result in direct or indirect remuneration to the University of Northern Colorado from a third party.

_____ _____

Signature of Patient or Personal Representative | Date

_____ _____

Print Name of Patient or Personal Representative | Description of Personal Representative's authority and attach document evidencing authority, such as a Power of Attorney

FAX COVER SHEET
****CONFIDENTIAL FACSIMILE++++

Name of Practice

University of Northern Colorado
Student Health Center/Counseling Clinic/Speech and Audiology Clinic
Telephone #: _____
FAX #: _____

TO: FROM:
Recipient: _____ Sender: _____

Fax Number: _____ Sender's Signature: _____

Telephone Number: _____ Sender's Phone Number: _____

No. of Pages (Including Cover) _____ Patient's Name: _____

Date of Transmission: _____ Medical Record #: _____

Name of Staff Member Authorizing Release: _____

Reason for release (select one):

Γ Patient Signed Consent Γ Medical Consultant

Γ Emergency Medical Care Γ Patient Transfer

Γ Travel Arrangements Γ Continued Patient Care

Γ Facilitate Payment Γ Facilitate Healthcare Operations

Information released (check all that apply)

Date Range of Materials Released: From _____ To _____

Γ Flow Sheets Γ General Reports Γ Measurements Γ Lab Results

Γ Therapy Report Γ Rehabilitation Γ Progress Notes

Γ Diagnostic Report Γ Progress Notes Γ Consultations

Γ Referral Γ Other _____