University of Montana Policies & Procedures implementing the Health Insurance Portability and Accountability Act Of 1996 (HIPAA)

Table of Contents

THE UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

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.

Certain "covered" entities within The University of Montana must maintain the privacy of your personal health information. These "covered" entities include the Curry Health Center, the Health Center Pharmacy, MonTECH, the New Directions Program, the Rhinehart Athletic Training Center, the UM Physical Therapy Clinic, and the DeWit Speech, Language, and Hearing Clinic. This notice describes how your protected health information about treatment, payment, health care operations, or for other purposes that are permitted or required may be used or disclosed. It also describes your rights to access and control your protected health information. Please note that all your personal health information will be available for release to you, to a provider regarding your treatment, or to certain other entities as required by law.

The "covered" entities within The University of Montana are required to abide by the terms of the Notice of Privacy Practices. However, the University reserves the right to change the privacy practices described in this notice, in accordance with the law. Changes to the privacy practices would apply to all health information maintained in the "covered" entities. If the privacy practices are changed, you may receive a revised copy of the privacy notice by contacting The University of Montana Chief Privacy Officer, Claudia Eccles, in the Office of Legal Counsel UH 132, 406-243-4755, Claudia.Eccles@umontana.edu.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Uses and Disclosures of Protected Health Information Based Upon Your Consent of Written Privacy Notice

Before you are provided with health care by a "covered" entity, you will be asked to sign a form acknowledging your receipt of this Privacy Notice. Once you have signed the acknowledgement form, you consent to the provisions of this Privacy Notice and your health information may be used and disclosed for the following purposes:

1. **Treatment.** Health care providers may use the information in your medical record to determine which treatment options best address your health needs. For example, your protected health information may be used to provide, coordinate, or manage your health care. This may include disclosure of your protected health information to a home health agency or to a pharmacy or medical equipment provider. In addition, your protected health information

may be disclosed to a specialist or a laboratory, which becomes involved with your health care diagnosis or treatment.

2. **Payment.** In order for an insurance company to pay for your treatment, a bill that identifies you, your diagnosis, and the treatment provided to you must be submitted. Such health information will be passed to an insurer in order to help receive payment for your medical bills.

3. **Health Care Operations.** Your diagnosis, treatment, and outcome information may be needed in order to improve the quality or cost of health care delivered. These quality and cost improvement activities may include evaluating the performance of your health care providers or examining the effectiveness of treatment provided to you.

In addition, your health information may be used for appointment reminders. For example, your medical record may be used to determine the date and time of your next appointment so a reminder can be sent or a telephone call made to remind you of the appointment. Also, your medical information may be examined to decide if another treatment or a new service may help you.

NOTE: If you refuse to provide your consent, treatment may be refused.[1]

<u>Uses and Disclosures of Protected Health Information That Can Be Made *Without* Your Written Consent</u>

1. **As required or permitted by law.** Some types of health information must be reported to legal authorities, such as law enforcement officials, court officials, or government agencies. For example, abuse, neglect, domestic violence or certain physical injuries may have to be reported. Also, responses to court orders are mandated by law.

2. **For public health activities.** Certain health authorities may require reporting of your health information to prevent or control disease, injury, or disability. This may include using your medical record to report certain diseases, injuries, birth or death information, information of concern to the Food and Drug Administration, or information related to child abuse or neglect. Also, certain work-related injuries may need to be reported to your employer so that your workplace can be monitored for safety.

3. **For health oversight activities.** Your health information may be disclosed to authorities so they can monitor, investigate, inspect, discipline or license those who work in the health care system or for government benefit programs.

4. **For activities related to death.** Your health information may be disclosed to coroners, medical examiners and funeral directors so they can carry out their duties related to your

[1] CFR § 164.506(b) (2001).

death, such as identifying the body, determining the cause of death or, in the case of funeral directors, to carry out funeral preparation activities.

5. **For organ, eye or tissue donation.** Your health information may be disclosed to people involved with obtaining, storing or transplanting organs, eyes or tissue of cadavers for donation purposes.

6. **For research.** Under certain circumstances, and only after a special approval process that usually involves removal of identifiers from disclosed information, your health information may be disclosed to help conduct research.

7. **To avoid a serious threat to health or safety.** As required by law and standards of ethical conduct, your health information may be disclosed to the proper authorities if, in good faith, it is believed that such release is necessary to prevent or minimize a serious and approaching threat to you or the public's safety.

8. **For military, national security, or incarceration/law enforcement custody.** If you are involved with the military, national security or intelligence agencies, or you are in the custody of law enforcement officials or an inmate in a correctional institution, your health information may be released to the proper authorities so that they may carry out their duties under the law.

9. **For worker's compensation.** Your health information may be disclosed to the appropriate persons to comply with laws related to worker's compensation or other similar programs. These programs may provide benefits for work-related injuries or illness.

10. **To those involved with your care or payment of care.** If people such as family members, relatives, or close personal friends are helping care for you or helping you pay your medical bills, important health information about you may be released to those people. You have the right to object to such disclosure, unless you are unable to function or there is an emergency.

NOTE: Except for the situations listed above, your specific, written authorization must be obtained for any other release of your health information. An authorization is different than consent. One primary difference is that, unlike cases with consents, a provider must treat you even if you do not wish to sign an authorization form.[2] If you sign an authorization form, you may withdraw your authorization at any time, as long as your withdrawal is in writing. If you wish to withdraw your authorization, please submit your written withdrawal to the covered entity to which you submitted the authorization (the Curry Health Center, the Health Center Pharmacy,

[2] 45 CFR § 164.508(e)(ii) (2001).

MonTECH, the New Directions Program, the Rhinehart Athletic Training Center, the UM Physical Therapy Clinic, and the DeWit Speech, Language, and Hearing Clinic).

YOUR HEALTH INFORMATION RIGHTS

You have several rights with regard to your health information. If you wish to exercise any of the following rights, please contact The University of Montana Chief Privacy Officer, Claudia Eccles, in the Office of Legal Counsel UH 132, 406-243-4755. Specifically, you have the right to:

1. **Inspect and obtain a copy of your health information.** With a few exceptions, you have the right to inspect and obtain a copy of your health information. However, this right does not apply to psychotherapy notes or information gathered for judicial proceedings, for example. In addition, a reasonable fee may be charged if you request a copy of your health information.

2. **Request to correct your health information.** If you believe your health information is incorrect, you may ask that the information be corrected. You should make such requests in writing and give a reason why your health information should be changed. However, your request may be denied if covered entities at The University of Montana did not create the health information you believe is incorrect or if these entities believe your information is correct.

3. **Request restrictions on certain uses and disclosures.** You have the right to ask for restrictions on how your health information is used or to whom your information is disclosed, even if the restriction affects your treatment, payment, or health care operation activities. Or, you may want to limit the health information provided to family or friends involved in your care or payment of medical bills. You may also want to limit the health information provided to authorities involved in disaster relief efforts. However, The University of Montana is not required to agree to your requested restrictions in all circumstances.

   If you receive certain medical devices (for example, life-supportive devices used outside a covered entity's facility), you may refuse to release or may restrict the release of your name, telephone number, social security number or other identifying information for purpose of tracking the medical device.

4. **As applicable, receive confidential communication of health information.** You have the right to ask that your health information be communicated to you in different ways or places. For example, you may wish to receive information about your health status in a special, private room or through a written letter to a private address. Reasonable requests for confidentiality made by you must be accommodated by the health care provider.

5. **Receive a record of disclosures of your health information.** In some limited instances, you have the right to ask for a list of the disclosures of your health information made from

covered entities in The University of Montana during the previous six years, but the request cannot include dates before April 14, 2003. This list must include the date of each disclosure, who received the disclosed health information, a brief description of the health information disclosed, and why the disclosure was made. The covered entities must comply with your request for a list within 60 days, unless you agree to a 30-day extension, and there will be no charge for the list, unless you request such a list more than once per year. In addition, the list of disclosures will not include disclosures made to you, or for purposes of treatment, payment, health care operations, inclusion in the entity's directory, or for national security, law enforcement/corrections, and certain health oversight activities.

6. **Obtain a paper copy of this notice.** Upon request, you may at any time receive a paper copy of this notice, even if you earlier agreed to receive this notice electronically.

7. **Complaints.** If you believe that your privacy rights have been violated, you may file a complaint with The University of Montana and with the federal Department of Health and Human Services. The University of Montana will not retaliate against you for filing such a complaint. To file a complaint, please contact The University of Montana Chief Privacy Officer, Claudia Eccles, in the Office of Legal Counsel UH 132, 406-243-4755, Claudia.Eccles@umontana.edu. She will provide you with the necessary assistance and paperwork.

Again, if you have any questions or concerns regarding your privacy rights or the information in this notice, please contact the University of Montana Chief Privacy Officer, Claudia Eccles, in the Office of Legal Counsel, UH 132, 406-243-4755.

This Notice of Medical Information Privacy is Effective April 14, 2003.

ISSUING AND ADMINISTERING PRIVACY NOTICE

Background

HIPAA privacy regulations require health care providers to notify patients of how the patient's health information may be used and disclosed, and the patient's rights and provider's legal duties with regard to their health information.

If the provider is in a direct treatment relationship with the patient (e.g., not providing care under the orders of another provider), then the provider must provide the privacy notice to the patient no later than the date of the first service delivery after the compliance date.

Policy

The University of Montana must:

1. Have the notice available at the service delivery site for patients to request to take with them;

2. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice;

3. Make a reasonable effort to assure that each patient gets a Notice of Privacy Practice at the first office visit after 4/13/03 and get written documentation from the patient that he/she received this notice;

4. Post the Privacy Notice on the covered entity's website, if applicable; and

5. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the above two requirements.

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

PATIENT ACKNOWLEDGEMENT OF RECEIVING "NOTICE OF PRIVACY PRACTICES"

I _____ (printed name of patient) hereby acknowledge on _____ I received from The University of Montana a printed copy of the Notice of Privacy Practices.

_____ /s/

_____ Date

BUSINESS ASSOCIATES WITH ACCESS TO PROTECTED HEALTH INFORMATION

Policy

Business Associate is a person or entity who provides certain functions, activities, or services, including the use and/or disclosure of Protected Health Information (PHI).

The University of Montana (UM) protects the confidentiality and integrity of confidential medical information as required by professional ethics and state and federal law.

UM is not liable for privacy violations of its business associates and is not required to actively monitor or oversee the means by which its business associates carry out safeguards, or the extent to which the business associates abide by the requirements of the contract. However, UM is required to act if it becomes aware of a practice or pattern that constitutes a material breach of the contract.

Standards and Procedure

UM must enter into contracts with its business associates containing language that the business associate will:

1. Not use or further disclose the information other than permitted or provided by the contract or required by law,
2. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for in its contract,
3. Report to UM any use or disclosure of the information not provided for by its contract of which it becomes aware,
4. Ensure any agents, including a subcontractor, to whom it provides PHI created by, or received from, or on behalf of UM, agree to the same conditions and restrictions that apply to the business associate with respect to such information,
5. Make PHI available in accordance with the UM policy on patients' access to PHI,
6. Make PHI available for amendment and incorporate amendments to PHI in accordance with UM policy on patients' right to amend or correct PHI,
7. Make available the information required to provide an accounting of disclosures in accordance with the UM policy on Accounting of Disclosures of PHI,
8. Make its internal practices, books, and records related to the use and disclosure of PHI received from, or created by, or on behalf of UM available to the U.S. Dept. of Health and Human Services (HHS) for the purposes of determining UM's compliance,
9. At the termination of its contract, if feasible, return or destroy all PHI received from, or created by, or on behalf of UM that the business associate retains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses or disclosures to those purposes that make the return or destruction infeasible.

In the event that UM becomes aware of a practice or pattern of the business associate that constitutes a material breach or a violation of the business associate's obligations under the contract, UM must take reasonable steps to cure the breach or end the violation, as applicable.

In the event that the business associate cannot or will not remedy the practice or pattern, UM must terminate the contract, if feasible. Where not feasible, contact The University of Montana Privacy Officer, Claudia Denker, in the Office of Legal Counsel, UH 132, 406-243-4755, Claudia.Eccles@umontana.edu, for reporting to HHS, as applicable.

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Addendum ("Addendum") amends and is hereby incorporated into the existing agreement known as _____ ("Agreement"), entered into by and between _____ (hereinafter "Business Associate") and The University of Montana (hereinafter "UM") on _____.

UM and Business Associate mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and HIPAA's implementing regulations, Title 45, Parts 160 and 164 of the Code of Federal Regulations ("Privacy Rule"), dealing with the confidentiality of health or health-related information. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

Definitions:

a. Protected Health Information (PHI) means any information, whether oral or recorded in any form or medium, that:
   (i) relates to the past, present or future physical or mental condition of any Individual; the provision of health care to an Individual; or the past, present or future payment of the provision of health care to an Individual; and
   (ii) identifies the Individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. PHI includes demographic information unless such information is de-identified according to the Privacy Rule.

b. Individual means the person who is the subject of PHI, and shall include a person who qualifies under the Privacy Rule as a personal representative of the Individual.

c. Capitalized terms used in this Agreement, but not otherwise defined, shall have the same meaning as those terms in the Privacy Rule.

Prohibition on Unauthorized Use or Disclosure of PHI: Business Associate shall not use or disclose any PHI received from or on behalf of UM except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by UM.

Use and Disclosure of Protected Health Information: Except as described in Section 4, Business Associate may use or disclose PHI only for the following purpose(s):

a. As necessary to perform its obligations under the Agreement.

b. As may be permitted in an attached Exhibit.

Use of PHI for Certain of Business Associate's Operations: Business Associate may use

and/or disclose PHI it creates for, or receives from, UM to the extent necessary for Business Associate's proper management and administration, or to carry out Business Associate's legal responsibilities, only if:

a. The disclosure is required by law; or

b. Business Associate obtains reasonable assurances, evidenced by written contract, from any person or organization to which Business Associate shall disclose such PHI that such person or organization shall:
   (i) hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization, or as required by law; and
   (ii) notify Business Associate, who shall in turn promptly notify UM, of any instance which the person or organization becomes aware of in which the confidentiality of such PHI was breached.

Safeguarding of PHI: Business Associate shall develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to prevent the improper use or disclosure of all PHI, in any form or media, received from or created or received by Business Associate on behalf of, UM Business Associate shall document and keep these security measures current.

Subcontractors and Agents: If Business Associate provides any PHI which was received from, or created for, UM to a subcontractor or agent, then Business Associate shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Business Associate by this Addendum.

Maintenance of the Security of Electronic Information: Business Associate shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Health Information received from, or on behalf of, UM which pertains to an Individual. Business Associate shall document and keep these security measures current and available for inspection, upon request. Business Associate's security measures must be consistent with HIPAA's Security regulations, Title 45, Part 142 of the Code of Federal Regulations ("Security Rule"), once these regulations are effective.

Compliance with Electronic Transactions and Code Set Standards: If Business Associate conducts any Standard Transaction for, or on behalf, of UM, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulation. Business Associate shall not enter into, or permit its subcontractors or agents to enter into, any Agreement in connection with the conduct of Standard Transactions for or on behalf of UM that:

a. changes the definition, Health Information condition, or use of a Health Information element;

b. adds any Health Information elements or segments to the maximum defined Health Information Set;

c. uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s); or

d. changes the meaning or intent of the Standard's Implementations Specification(s).

Access to PHI: At the direction of UM, Business Associate agrees to provide access to any PHI held by Business Associate which UM has determined to be part of UM's Designated Record Set, in the time and manner designated by UM. This access will be provided to UM or, as directed by UM, to an Individual, in order to meet the requirements under the Privacy Rule.

Amendment or Correction to PHI: At the direction of UM, Business Associate agrees to amend or correct PHI held by Business Associate and which UM has determined to be part of UM's Designated Record Set, in the time and manner designated by UM.

Reporting of Unauthorized Disclosures or Misuse of PHI: Business Associate shall report to UM any use or disclosure of PHI not authorized by this Addendum or in writing by UM. Business Associate shall make the report to UM's Privacy Official not less than one (1) business day after Business Associate learns of such use or disclosure. Business Associate's report shall identify:

(i) the nature of the unauthorized use or disclosure,
(ii) the PHI used or disclosed,
(iii) who made the unauthorized use or received the unauthorized disclosure,
(iv) what Business Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
(v) what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure. Business Associate shall provide such other information, including a written report, as reasonably requested by UM's Privacy Official.

Mitigating Effect of Unauthorized Disclosures or Misuse of PHI: Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a misuse or unauthorized disclosure of PHI by Business Associate in violation of the requirements of this Addendum.

Tracking and Accounting of Disclosures: So that UM may meet its accounting obligations under the Privacy Rule,

a. Disclosure Tracking: Starting April 14, 2003, for each disclosure not excepted under subsection (b) below, Business Associate will record for each disclosure of PHI it makes to UM or a third party of PHI that Business Associate creates or receives for or from UM:
   (i) the disclosure date,
   (ii) the name and (if known) address of the person or entity to whom Business Associate made the disclosure,
   (iii) a brief description of the PHI disclosed, and

(iv) a brief statement of the purpose of the disclosure.

For repetitive disclosures which Business Associate makes to the same person or entity, including UM, for a single purpose, Business Associate may provide:

(i) the disclosure information for the first of these repetitive disclosures,
(ii) the frequency, periodicity or number of these repetitive disclosures, and
(iii) the date of the last of these repetitive disclosures. Business Associate will make this log of disclosure information available to UM within five (5) business days of the UM's request.

b. Exceptions from Disclosure Tracking: Business Associate need not record disclosure information or otherwise account for disclosures of PHI that meet each of the following conditions:

(i) the disclosures are permitted under this Addendum, or are expressly authorized by UM in another writing; and,
(ii) the disclosure is for one of the following purposes:
   a. UM's Treatment, Payment, or Health Care Operations;
   b. in response to a request from the Individual who is the subject of the disclosed PHI, or to that Individual's Personal Representative;
   c. made to persons involved in that individual's health care or payment for health care;
   d. for notification for disaster relief purposes;
   e. for national security or intelligence purposes; or,
   f. to law enforcement officials or correctional institutions regarding inmates.

c. Disclosure Tracking Time Periods: Business Associate must have available for UM the disclosure information required by this section for the six-year period preceding UM's request for the disclosure information (except) Business Associate need have no disclosure information for disclosures occurring before April 14, 2003).

Accounting to Covered Entity and to Government Agencies: Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from or on behalf of, or created for, UM available to UM, or at the request of UM, to the Secretary of the Department of Health and Human Services (HHS) or his/her designee, in a time and manner designated by UM or the Secretary or his/her designee, for the purpose of determining UM's compliance with the Privacy Rule. Business Associate shall promptly notify UM of communications with HHS regarding PHI provided by or created by UM and shall provide UM with copies of any information Business Associate has made available to HHS under this provision.

Term and Termination:

a. This Addendum shall take effect April 14, 2003.

b. In addition to the rights of the parties established by the underlying Agreement, if UM reasonably determines in good faith that Business Associate has materially breached any of its obligations under this Addendum, Covered Entity, in its sole discretion, shall

have the right to:

(i) exercise any of its rights to reports, access and inspection under this Addendum; and/or

(ii) require Business Associate to submit to a plan of monitoring and reporting, as UM may determine necessary to maintain compliance with this Addendum; and/or

(iii) provide Business Associate with a _____ day period to cure the breach; or

(iv) terminate the Agreement immediately.

c. Before exercising any of these options, UM shall provide written notice to Business Associate describing the violation and the action it intends to take.

Return or Destruction of PHI: Upon termination, cancellation, expiration or other conclusion of the Agreement, Business Associate shall:

a. Return to UM or, if return is not feasible, destroy all PHI and all Health Information in whatever form or medium that Business Associate received from or created on behalf of UM. This provision shall also apply to all PHI that is in the possession of subcontractors or agents of Business Associate. In such case, Business Associate shall retain no copies of such information, including any compilations derived from and allowing identification of PHI. Business Associate shall complete such return or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Business Associate shall certify on oath in writing to UM that such return or destruction has been completed.

b. If Business Associate believes that the return or destruction of PHI or Health Information is not feasible, Business Associate shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, Business Associate shall extend the protections of this Addendum to PHI and Health Information received from or created on behalf of UM, and limit further uses and disclosures of such PHI, for so long as Business Associate maintains the PHI.

Miscellaneous:

a. Automatic Amendment: Upon the effective date of any amendment to the regulations promulgated by HHS with regard to PHI, this Addendum shall automatically amend so that the obligations imposed on Business Associate remain in compliance with such regulations.

b. Interpretation: Any ambiguity in this Addendum shall be resolved in favor of a meaning that permits UM to comply with the Privacy Rule.

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

THE UNIVERSITY OF MONTANA	BUSINESS ASSOCIATE
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____

TREATMENT, PAYMENT & HEALTH CARE OPERATIONS AS DEFINED BY HIPAA

TREATMENT

Treatment activities are those taken on behalf of a single individual – not an entire population. Only health care providers can deliver treatment, not group health plans or employers (in their role as an employer). Some activities, such as telephone nursing assistance, would be "treatment" if provided by a health care provider or "health care operations" if provided by a group health plan. Treatment includes:

- Providing, coordinating, or managing health care and related services by one or more health care providers;
- Coordinating or managing health care with a third party;
- Consulting between health care providers to provide care to an individual;
- Referring the individual to another health care provider.

PAYMENT

Payment includes all activities undertaken by a health care provider to get reimbursement for services provided to an individual. Payment includes:

- Determining the eligibility or coverage of an individual's benefits;
- Billing, claims management, collection activities and related data and information processing activities;
- Utilization review activities – including pre-certifying and preauthorizing services, concurrent and retrospective review of services provided;
- Disclosures to consumer reporting agencies for either collection of premiums or reimbursement. Health care provider may disclose:
    - Name and address;
    - Date of birth;
    - Social security number;
    - Payment history;
    - Account number;
    - Name and address of the health care provider and/or health plan;

HEALTH CARE OPERATIONS

Health care operations include any of the following activities done as a Covered Entity (CE) (if the CE has components that are not CE's):

- Conducting quality assessment & improvement activities, including outcomes evaluation and development of clinical guidelines, so long as such activities are not part of a research study (research is covered under separate IRB guidelines);
- Reviewing the competence and qualifications of health care professionals and evaluating their performance;
- Conducting training programs for students & interns to learn under supervision & practice or improve their skills as health care providers;
- Training health and non-health care professional employees;
- Accreditation, certification, licensing or credentialing activities;
- Conducting or arranging medical review, legal services and auditing functions – including fraud and abuse detection and compliance programs;
- Business planning and development – including cost-management and planning related analyses related to managing the group health plan. This may include developing and administrating the drug formulary; and developing or improving methods of payment or coverage policies;
- General management and administration, including;

    - Any management activities relating to implementing and complying with the Privacy Rule;
    - Customer service;
    - Resolving internal grievances with employees or patients;
    - Selling, transferring, merging or consolidating any part of or all of the group health plan;

USE AND DISCLOSURE BY AND FOR PERSONAL REPRESENTATIVES, MINORS, AND DECEASED INDIVIDUALS

Policy

A Personal Representative is treated as the individual. The personal representative (PR) may be any adult who has decision-making capacity and who is willing to act on behalf of the patient. A PR may include an individual who has lawful authority to act in the place of the individual. This includes parents, legal guardians or properly appointed agents designated by Montana law.

A minor is an individual under the age of 18 who has not been legally emancipated by a court and is:

1. Not legally or previously married,
2. Without children,
3. Not a high school graduate,
4. Not separated from parents and self-supporting,
5. Not pregnant or carrying a communicable disease,
6. Not in need of emergency care without which the minor's health would be at stake.

Unemancipated minors, incapacitated and deceased individuals must have a PR identified in order to provide acknowledgment of the *Notice of Privacy Policy* or *Authorization to Use and Disclose PHI*. Once a minor is emancipated, a guardian or parent cannot be recognized as a personal representative.

The University of Montana does not have to recognize a PR as the individual, if the PR is suspected of abusing, neglecting or endangering the individual.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR WORKERS' COMPENSATION PURPOSES

Background

In compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The University of Montana may disclose protected health information (PHI) to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault. However, the health information disclosed must be limited to the minimum amount necessary to carry out the purpose of the disclosure and must be limited to that which is relevant to the individual's condition under consideration.

An employee filing a claim for workers' compensation due to an on-the-job injury consents to certain conditions. One of those conditions is, at the employer's request, they will submit to an examination to determine the validity of their claim. This information is then available, with certain restrictions, to the employee, employer, Department of Workforce Development, or representative of any of these to assist in resolving the claim.

Employees filing a workers' compensation claim waive all provider-patient privilege of information or results regarding any condition or complaint **reasonably related to the condition that they are claiming compensation for.** This includes information normally covered by any applicable law, but only if it is related to the condition that the employee is seeking compensation for.

Procedures

1. Copies of medical records or verbal communications, reasonably related to a work injury, should be released within a reasonable time, after written request, to the employee, employer, workers compensation insurance carrier for the employer, Department of Labor and Industry or its representative.

2. Requests for copies of medical records which extend beyond the scope of the work-related injury need to be accompanied by a written authorization from the patient/employee.

3. Providers furnish legible duplicates of written material requested. Certified copies are furnished upon request. Refusal to provide the requested copies can result in the provider being liable for all costs of preparing the records and attorney's fees incurred while attempting to get the requested copies.

4. Fees for copies are set by State statute, with a limit of the greater of $7.50 per request or

$.45 per page plus the actual postage cost.

5. Records of the Department of Labor and Industry which identify an employee filing a worker's compensation claim are confidential and not subject to inspection or copying. This includes the following:

   Identifying the employee

   Disclosing the nature of the claimed injury

   Disclosing past or present medical condition

   Describing the extent of disability

   Disclosing the amount, type or duration of any benefits provided to the employee

   Disclosing any financial information provided to the department by self-insured employer or person applying for exemption

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

Purpose

To ensure The University of Montana employees understand when and how to disclose a patient's personal health information (PHI) in relation to judicial and administrative proceedings.

Background

There may be instances where a patient is involved with a legal proceeding, either conducted by a court of law (such as a state trial court or federal district court) or a government agency (such as a state Department of Health and Family Services or the federal Centers for Medicare and Medicaid Services).

In these legal proceedings, lawyers, judges and others involved with the proceeding may contact The University of Montana to access the patient's PHI. Examples of health information these proceedings may require include information about a certain medical procedure the patient underwent to determine whether the procedure is covered under a health plan or the outcome of that procedure, results of blood or genetic tests in child custody or similar proceedings, medical records that document disabling conditions in discrimination cases, or health information that documents serious illnesses for conflicts pertaining to medical leave**.**

Policy

The University of Montana may disclose PHI in the course of any judicial or administrative proceeding:

a. in response to an order from a court or administrative tribunal.

b. in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal.

Procedure for disclosing PHI in response to a court/administrative order

If The University of Montana receives an order from a court or administrative judge, only release the PHI which the order expressly authorizes to be disclosed and the request is relevant and material to a legitimate legal inquiry; the request is specific and limited in scope to the extent necessary; and de-identified information could not be used.

Procedure for disclosing PHI in response to a subpoena, discovery request or other lawful process (other than a court order)

We may only release PHI in such instances if at least **one of the following three** events has occurred:

I. We may release PHI if we receive ***written*** satisfactory assurance from the party requesting the information that reasonable efforts have been made by such party to ensure that the patient who is the subject of the PHI has been given notice of the request.

A. Satisfactory assurance that the requesting party has tried to notify the patient of the PHI request means the following:

1. the requesting party has given The University of Montana a *written statement and accompanying documentation* demonstrating that:

2. the requesting party has made a good faith attempt to provide written notice to the patient (if the patient's location is unknown, documentation showing that a notice was mailed to the patient's last known address);

3. the notice provided by the requesting party to the patient contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI.

4. the time for the patient to raise objections to the court or administrative tribunal has passed and either no objections were filed, or all objections filed by the patient have been resolved and the disclosures being sought are consistent with the court's resolution.

II. We may also release PHI to a requesting party if we receive ***written*** satisfactory assurance from the requesting party that reasonable efforts have been made by such party to secure a *qualified protective order*. A *qualified protective order* is an order of a court or administrative tribunal or a stipulation by the parties to the proceeding that prohibits the parties from using or disclosing PHI for any purpose other than the proceeding for which the information was requested and requires the parties to return the PHI (including all copies made) to The University of Montana at the end of the proceeding.

A. Satisfactory assurance in this instance means that we have received from the requesting party a written statement and accompanying documentation demonstrating that:

1. the parties to the dispute giving rise to the request for PHI have *agreed* to a qualified protective order and have presented it to a court or administrative tribunal with jurisdiction over the dispute; **OR**

2. the requesting party has asked for a qualified protective order from such court or administrative tribunal.

III. We may release PHI to a requesting party even without satisfactory assurance from that party if we, The University of Montana, either:

A. Make reasonable efforts to provide notice to the patient about releasing his or her PHI, so long as the notice meets all of the following requirements:

1. the notice is written and given to the patient (if the patient's location is unknown, we should establish documentation showing that a notice was mailed to the patient's last known address);

2. the notice contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI;

3. the time for the patient to raise objections to the court or administrative tribunal has elapsed and either no objections were filed, or all objections filed by the patient have been resolved and the disclosures being sought are consistent with the court's resolution;
OR

B. Seek a qualified protective order from the court or administrative tribunal or convince the parties to stipulate to such order.

DISCLOSURE TO THIRD PARTIES

Policy

The University of Montana (UM) may use and disclose certain PHI without the written consent or authorization to release the information from the individual. The individual must be informed in advance of the use or disclosure and have the opportunity to agree, prohibit, or restrict the disclosure.

UM may disclose to family members, other relatives, close personal friends, clergy, or others identified by an individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. UM may use or disclose PHI to notify or assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual or the individual's location, general condition, or death. The individual's presence is a determining factor in order to use or disclose PHI for these purposes.

Use and Disclosure with the Individual Present:

If an individual is present or otherwise available prior to a use or disclosure and has the capacity to make health care decisions, UM may use or disclose the PHI if it:

1. Obtains the individual's agreement;
2. Provides the individual opportunity to object to use or disclosure, and the individual does not express an objection; or
3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to such disclosure.

Limited Uses and Disclosures when the Individual is not Present:

If the individual is not present or the opportunity to agree or object to the use or disclosure cannot practically be provided due to the individual's incapacity or an emergency circumstance, UM may, in exercise of professional judgment, determine whether the disclosure is in the individual's best interest and, if so, disclose only the PHI which is directly relevant to that person's involvement with the individual's health care. UM may use professional judgment and its experience of common practice to make reasonable inferences of the individual's best interests in allowing a person to act on the individual's behalf to pick up filled prescriptions, X-rays, medical supplies, or other similar forms of PHI.

USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR MARKETING PURPOSES

Policy

It is the policy of The University of Montana to secure an authorization to use or disclose protected health information (PHI) for marketing purposes in compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. [164.501, 164.508(a)(3)]

Definition

Per 164.501, marketing is defined as:

1. to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service; or

2. an arrangement involving a covered entity whereby PHI is disclosed by the covered entity in exchange for direct or indirect remuneration, so that the other entity or affiliate can make a communication that encourages the purchase or use of its own product or service.

The following are examples of situations that do not meet the definition of marketing

1. Communications that are merely promoting good health and not about a specific product or service does not meet the definition of marketing. So mailings reminding women to get an annual mammogram, or with information about how to lower cholesterol, about new developments in health care like new diagnostic tools or about health or wellness classes, support groups and health fairs are permitted and not considered marketing.

2. Communications about government-sponsored programs do not fall within the definition of marketing. There is no commercial component to communications about benefits available through public programs, so The University of Montana is permitted to use/disclose PHI to communicate about eligibility for Medicare supplement benefits, or SCHIP.

3. The University of Montana may make communications in newsletter format without authorization so long as the content of such does not fit the definition of marketing.

Exceptions to the Scope of Marketing Activities so Authorization is not needed

Marketing does not include:

1. oral or written communications that describe The University of Montana network or covered services; or

2. communications about treatment for the patient; or

3. communications about case management or care coordination, or recommendations of treatment alternatives and care options, including health care providers or settings of care.

The following are examples of these exceptions

1. The University of Montana can convey information to beneficiaries and members about health insurance products offered by The University of Montana that could enhance or substitute for existing health plan coverage. For example, if a child is about to age out of coverage under a family's policy, this provision will allow the plan to send the family information about continuation coverage for the child. This does NOT extend to excepted benefits such as accident-only policies or to other lines of insurance.

2. Doctors can write a prescription or refer an individual to a specialist for follow-up tests because these are communications about treatment.

Procedure for Authorization to Use or Disclose PHI for Marketing Purposes

1. The University of Montana will obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of a face-to-face communication with the patient; or a promotional gift of nominal value provided by a covered entity.

2. If the marketing involves The University of Montana receiving direct or indirect remuneration by a third party, the authorization will state that such remuneration is involved.

The following are examples of situations that require authorization

1. NPRM clearly states that nothing in the Final Rule will permit a covered entity to sell lists of patients or enrollees to third parties or to disclose PHI to a third party for the independent marketing activities of the third party. A pharmaceutical company cannot pay a provider for a list of patients with a particular condition or taking a particular medication and then use that list to market its own drug products directly to those patients.

PATIENT PHOTOGRAPHY, VIDEOTAPING, OTHER IMAGING, AND AUDIO RECORDING

Policy

The University of Montana may use a variety of media to collect health information and obtain the patient's informed consent in writing before creating photographs, videotapes, other images, or audio recordings of the patient.

"Consent" means written documentation of the patient's agreement to be photographed, videotaped, otherwise imaged, or recorded. Written consent establishes a reliable record of patient consent in case consent is later questioned. Written consents become part of the patient's health care record.

Consents are valid for only a reasonable period of time, e.g. the duration of the immediate health concern. A new consent should be obtained if the situation surrounding the imaging or recording has changed.

In addition, the patient has the right to withdraw the consent at any time, provided the withdrawal is in writing. Photographs, videotapes, other images, and audio recordings, which were obtained before the patient withdrew consent, are part of the patient's health record and shall be maintained according to The University of Montana's retention of records policy.

Procedures

1. Except under very limited circumstances (see 6.a. below), images and recordings may not be created for any purpose without the written consent of the patient.

2. As part of obtaining consent, the patient is given an explanation of:
    a. The purpose of the photographing, videotaping, imaging, or audio recording,

    b. Any proposed use of the images or recordings for commercial, educational, promotional or legal purposes,

    c. The security mechanisms to be used to protect patient privacy, and

    d. The duration of retention of the images recordings.
3. The University of Montana provides the patient with the above information in sufficient detail and understandable language to enable him or her to give informed consent to the proposed imaging or recording as a free and knowledgeable choice.

4. A health care provider (physician, registered nurse, physician assistant, psychologist, counselor, etc.) is responsible for providing the patient with an appropriate explanation of the imaging or recording and obtaining his or her informed consent in writing.
5. Circumstances that may involve patient imaging or recording include:

    a. Documentation of abuse and neglect: Reportable cases of actual or suspected abuse and neglect do not require consent from the patient prior to photography, videotaping, and other imaging. These images may be submitted to the investigating agency with appropriate authorization/court order, but are not to be used for other purposes without consent.

    b. Research: Consent for imaging or recording must be explicitly stated in the patient's consent for participation in the research protocol. The University of Montana's institutional review board or privacy board must approve the creation of images and recordings as part of a research protocol.

    c. Telemedicine (including e-mail) and Internet transmission: Consent for The University of Montana to use images or recordings for these purposes must be explicitly stated in the patient's written consent. The images or recordings, along with the medical record, should be encrypted in order to protect the patient's privacy.

    d. Medical education or teaching: Consent for The University of Montana to use images or recordings for these purposes must be explicitly stated in the patient's written consent.

    e. Marketing/Fundraising/Publicity/Media: Authorization/consent for The University of Montana to use images or recordings for these purposes must be explicitly stated in the patient's written authorization/consent.

    f. Law enforcement or legal purposes: Consent for The University of Montana to use images or recordings for these purposes must be explicitly stated in the patient's written consent.

    g. Videotaping for Trauma Certification/Performance Improvement Purposes: Videotaping as a documentation "tool" for peer review, performance improvement activities, or trauma certification may be carried out with patient authorization. However, viewing is limited to authorized staff as per The University of Montana guidelines. The videotapes are not considered a part of the patient's health information and will be erased following completion of the performance improvement process.

h. Photography of Newborns: Consent of the parent must be obtained prior to photographing of newborns as a courtesy or for sale.

i. Family/Friends: Documented consent is not needed for imaging or audio recording done by the patient's family members or friends. However, if a family member or friend has the consent of the patient to videotape a birth or procedure, for example, this should be done only with the agreement of the attending physician and acknowledgement that the individual may be required to discontinue taping if the attending physician deems it necessary.

7. The University of Montana may not release images and recordings to individuals outside The University of Montana without specific authorization from the patient, except when required by law or when the images or recordings have been "de-identified" and are no longer considered individually identifiable health information.

8. The University of Montana may determine that images and recordings are not individually identifiable health information only if identifiers, including full-face photographic images and any comparable ages of the individual or of relatives, employers, or household members of the individual, are removed. (See The University of Montana's *Destruction and Disposal of PHI* Policy.)

9. Storage and retention of images and recordings:

   a. Images and recordings must be clearly identified with the patient's name, identification number and/or date of birth, and date of image or recording. Media must be stored securely to protect the patient's confidentiality. If used to document patient care, images and recordings will be stored in compliance with The University of Montana's retention of records policy and state law.

   b. Still images and recordings created for medical purposes may be filed with the patient's health care record.

   c. Sensitive images and recordings may be stored in sealed envelopes within the patient's health care record.

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

PATIENT CONSENT/AUTHORIZATION

PHOTOGRAPHY/VIDEOTAPING/OTHER IMAGING/AUDIO RECORDING FOR TREATMENT, EDUCATION, MARKETING OR MEDIA PURPOSES

Patient Name:	**MR #:**
Address:	**Phone No:**

I hereby give my consent to have photographs, videotaped images, other images, or audio recordings made of my family member or myself for the following purposes:

☐ **Covered Entity Marketing or Publicity Purposes**
Event: _____

☐ **Interviews with News Media**
Covered Entity/s: _____

☐ **Educational Purposes:** _____

☐ **Other:** _____

Signature of Patient or Legal Representative/Relationship	**Date**
Witness	**Date**

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

Permission to Gather Personal Health Information (PHI)

There are two common approaches to gathering Personal Health Information (PHI): 1) directly from an individual or, if a minor, an individual's parent/guardian; and 2) requesting information from an entity such as the individual's healthcare provider, hospital, clinic, or health plan.

Directly from an individual: Principal Investigators asking research subjects to personally provide Personal Health Information (e.g., current health problems, current medications, past serious illness/injuries/surgeries, etc.), **may** include the following on the Informed Consent Form (or Parental Permission form), in addition to the standard ICF language:

Disclosure of Personal Health Information
My [My child's] individual health information that may be used to conduct this research includes:

*[**INSERT** list of all individual health information to be collected for this protocol/study, such as demographic information, results of physical exams, blood tests, x-rays, and other diagnostic and medical procedures, as well as medical history]*.

I authorize *[**INSERT** name of Principal Investigator]* and the researcher's staff *[OPTIONAL: and any collaborators, other clinical sites involved in this research, sponsors if applicable, outside laboratories]* to use my [my child's] individual health information for the purpose of conducting the research project entitled "*[**INSERT** title of study]*."

If I receive [my child receives] compensation for participating in this study, identifying information about me [my child] may be used as necessary to provide compensation.

Signature: _____ Date: _____

Requesting information from an entity: If asking permission to access research subjects' Personal Health Information (e.g., current health problems, current medications, past serious illness/injuries/surgeries, etc.) from an entity such the individuals' health provider, hospital, clinic, or health plan, the Principal Investigator **must** include the following form ("Authorization to Disclose Protected Health Information for Research Purposes") in addition to the Informed Consent Form or, in the case of a minor, the Parental Permission form.

Note: The IRB approval stamp must appear on both the ICF (and Parental Permission form, if appropriate) and HIPAA Authorization Form.

Attachment

Authorization to Use and Disclose Protected Health Information for Research Purposes

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

Authorization to Use and Disclose Protected Health Information for Research Purposes

---

Purpose: I authorize [***INSERT*** *name of entity with protected health information, e.g., health provider, hospital, clinic, health plan]* to disclose to *[**INSERT** name of PI]* the following protected health information:

> *[**INSERT** list of all individual health information to be collected for this protocol/study, such as demographic information, results of physical exams, blood tests, x-rays, and other diagnostic and medical procedures, as well as medical history]*.

This protected health information is to be used/disclosed by [***INSERT*** *name of PI]* and the researcher's staff *[OPTIONAL: and any collaborators, other clinical sites involved in this research, sponsors if applicable, outside laboratories]* only for the purpose of conducting the research project entitled *[**INSERT** title of study]*.

*[**INSERT** name of PI]* may use/disclose my existing protected health information (PHI), or any created within the next six (6) months for up to thirty (30) months from the date of my signing this authorization.

Right to Refuse: I may refuse to sign this authorization if I so choose. If I decide not to sign the Authorization, I will not be allowed to participate in this study or receive any research related treatment that is provided through the study. However, my decision not to sign this authorization will not affect my current or future other treatment, current or future payment, enrollment in health plans, or eligibility for benefits at The University of Montana (if applicable).

Right to Revoke: At all times, I retain the right to revoke this Authorization. Such revocation must be submitted in writing to [***INSERT*** *name of entity with protected health information, e.g., hospital, clinic, health provider, health plan]*. Withdrawal of this Authorization shall be effective *except* to the extent that [***INSERT*** *name of PI]* has already used or disclosed information released prior to receiving notice of the revocation.

Potential for Re-disclosure: I understand that once my health information is disclosed under this Authorization, there is a potential that it could be re-disclosed outside this study and no longer covered by this Authorization. I also understand that there are laws that may require my individual health information to be disclosed for public purposes, such as if required for mandated reporting of abuse or neglect, judicial proceedings, health oversight activities and public health measures.

This Authorization does not have an expiration date.

I am the research participant or personal representative authorized to act on behalf of the participant. I have read this information, and I will receive a copy of this authorization form after it is signed.

_____	_____
Signature of research participant or research participant's personal representative	Date
_____	_____
Printed name of research participant or research participant's personal representative	Description of personal representative's authority to act on behalf of research participant

PATIENT'S RIGHT TO ACCESS, INSPECT AND COPY PROTECTED HEALTH INFORMATION

Background

In compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), providers must have in place implemented policies and procedures to ensure patients' right to access, inspect and copy protected health information (164.524). An individual has the right to access their information in all but a limited number of situations, which include:

1. Psychotherapy notes;
2. Information compiled in anticipation of or use in a civil, criminal, or administrative action or proceeding;
3. Protected health information subject to the Clinical Laboratory Improvements Amendment (CLIA) of 1988.
4. Protected health information exempt from CLIA, pursuant to 42 CFR 493.3(a)(2). In other words, protected health information generated by 1) facilities or facility components that perform testing for forensic purposes; 2) research laboratories that test human specimens but do not report patient-specific results for diagnosis, prevention, treatment, or the assessment of the health of individual patients; 3) laboratories certified by the National Institutes on Drug Abuse (NIDA) in which drug testing is performed that meets NIDA guidelines and regulations.

In the situations above, The University of Montana may deny the individual access without providing an opportunity for review.

The University of Montana may also deny an individual access without providing an opportunity for review when:

1. The covered entity is a correctional institution or a healthcare provider acting under the direction of the correctional institution and an inmate's request to obtain a copy of protected health information would jeopardize the individual, other inmates, or the safety of any officer, employee, or other person at the correctional institution, or a person responsible for transporting the inmate;
2. The individual, when consenting to participate in research that includes treatment, agreed to temporary denial of access to protected health information created or obtained by a healthcare provider in the course of research, and the research is not yet complete;
3. The records are subject to the Privacy Act of 1974 and the denial of access meets the requirement of that law;
4. The protected health information was obtained from someone other than a healthcare

provider under a promise of confidentiality and access would likely reveal the source of the information.

The University of Montana may also deny an individual access under the following circumstances, provided that the individual is given a right to have such denials reviewed:

1. A licensed healthcare professional has determined that the access is likely to endanger the life or physical safety of the individual or another person;
2. The protected health information makes reference to another person who is not a healthcare provider, and a licensed healthcare professional has determined that the access request is reasonably likely to cause substantial harm to such other person;
3. The request for access is made by the individual's personal representative and a licensed healthcare professional has determined that access is reasonably likely to cause substantial harm to the individual or another person.

Detailed requirements for denial review are outlined in 45 CFR, Section 164.524. See also below, the section entitled Access, Inspection and/or Copy Request is Denied in Whole or in Part.

Policy

It is the policy of The University of Montana to honor a patient's right of access to inspect and obtain a copy of their protected health information (PHI) in the organization's designated record set, for as long as the PHI is maintained in compliance with HIPPA and the organization's retention policy.

Procedures

1. A patient must make a request to a staff member to access and inspect their protected health information. Whenever possible, this request shall be made in writing and documented on either the Authorization for Disclosure form or in the notes of the patient's health record.

2. Determination of accessibility of the information shall be based on:

    a. Criteria outlined above, as supported by State and Federal laws;
    b. Availability of protected patient information (i.e., final completion of information, long term storage, retention practices, etc.)

3. The University of Montana must take action within 10 days after receipt of the request when the PHI is on-site, and within 21 days when the PHI is off-site or not immediately available, if The University of Montana provides the patient with a written statement of the reasons for the delay and the date by which the access request will be processed. If The University of Montana does not maintain the requested PHI, it must tell the requestor who does.

4. The University of Montana must document and retain the designated record sets subject to access, and the titles of persons or offices responsible for receiving and processing requests for access.

Access, Inspection and/or Copy Request is Granted

1. The patient and The University of Montana will arrange a mutually convenient time and place for the patient to inspect and/or obtain a copy of the requested PHI. Inspection and/or copying of PHI will be carried out within the organization with staff assistance.

2. The patient may choose to inspect the PHI, copy it, or both, in the form or format requested. If the PHI is not readily producible in the requested form or format, the organization must provide the patient with a readable hard copy form, or other form as agreed to by the organization and the patient.

    a. If the patient chooses to receive a copy of the PHI, the organization may offer to provide copying services. The patient may request that this copy be mailed.
    b. If the patient chooses to copy their own information, the organization may supervise the process to ensure that the integrity of the patient record is maintained.

3. Upon prior approval of the patient, the organization may provide a summary of the requested PHI.

4. The organization may charge a reasonable fee for the production of copies or a summary of PHI, if the patient has been informed of such charge and is willing to pay the charge.

5. If upon inspection of the PHI the patient feels it is inaccurate or incomplete, the patient has the right to request an amendment to the PHI. The organization shall process requests for amendment as outlined in additional organizational policy/procedures addressing this patient right.

Access, Inspection and/or Copy Request is Denied in Whole or in Part

1. The organization must provide a written denial to the patient. The denial must be in plain language and must contain:

    a. The basis for the denial;
    b. A statement, if applicable, of the patient's review rights; and
    c. A description of how the patient may complain to The University of Montana or to the Secretary of Health and Human Services.

2. If access is denied because The University of Montana does not maintain the PHI that is the subject of the request, and The University of Montana knows where the PHI is

maintained, The University of Montana must inform the patient where to direct the request for access.

3. The University of Montana must, to the extent possible, give the patient access to any other PHI requested, after excluding the PHI as to which The University of Montana has grounds to deny access.

4. If access is denied on a ground permitted under (HIPAA) 164.524, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by The University of Montana to act as a reviewing official and who did not participate in the original decision to deny.

5. The patient must initiate the review of a denial by making a request for review The University of Montana. If the patient has requested a review, The University of Montana must provide or deny access in accordance with the determination of the reviewing professional, who will make the determination within a reasonable period of time.

6. The University of Montana must promptly provide written notice to the patient of the determination of the reviewing professional. See #10 above for denial requirements.

PATIENT'S RIGHT TO REQUEST AMENDMENT OF PROTECTED HEALTH INFORMATION

Policy

It is the policy of The University of Montana to honor a patient's right to request an amendment or correction to their protected health information if they feel that the information is incomplete or inaccurate. The patient has the right to request an amendment of their protected health information for as long as that information is maintained in the designated record set.

Procedures

1. Patient requests for amendment of protected health information shall be made in writing to The University of Montana and clearly identify the information to be amended, as well as the reasons for the amendment. These requirements are detailed in the Notice of Privacy Practices.

2. Requests may be denied if the material requested to be amended:

    a. was not created by The University of Montana, unless the originator is no longer available to act on the request.
    b. is not part of the individual's health record.
    c. is not accessible to the individual because federal and state law do not permit it.
    d. is accurate and complete.

3. The University of Montana must act on the individual's request for amendment no later than 10 days after receipt of the amendment. The University of Montana may have up to 21 days for processing the amendment if the record is permanently or temporarily unavailable and if the individual is given a written statement of the reason for the delay, and the date by which the amendment request will be processed.

Amendment Request is Granted

4. If the request is **granted**, after review and approval by the individual responsible for the entry to be amended, The University of Montana must:

    a. Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment.
    b. Inform the individual that the amendment is accepted.

    c. Obtain the individual's identification of and agreement to have The University of Montana notify the relevant persons with whom the amendment needs to be shared.
    d. Within a reasonable time frame, make reasonable efforts to provide the amendment to persons identified by the individual, and persons, including business associates, that The University of Montana knows have the protected health information that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the individual.

Amendment Request is Denied

5. If the request is **denied**, The University of Montana must provide the individual with a timely manner, written denial in plain language that contains:

    a. The basis for the denial (see #2 above);
    b. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
    c. A statement that if the individual does not submit a statement of disagreement, the individual may request that The University of Montana provide the individual's request for amendment and the denial with any future disclosures of the protected health information that was the subject of the request.
    d. A description of how the individual may complain to the The University of Montana or the Secretary of Health and Human Services; and
    e. The name or title, and the telephone number of the designated contact person who handles complaints The University of Montana.

6. The University of Montana must permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such agreement. The University of Montana may reasonably limit the length of a statement of disagreement.

7. The University of Montana may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, The University of Montana must provide a copy to the individual who submitted the statement of disagreement.

8. The University of Montana must, as appropriate, identify the record of protected health information that is the subject of the disputed amendment and append or otherwise link the individual's request for amendment, The University of Montana's denial of the request, the individual's statement of disagreement, if any, and The University of Montana's rebuttal, if any.

9. If the statement of disagreement has been submitted by the individual, The University of Montana must include the material appended or an accurate summary of such information with any subsequent disclosure of the protected health information to which the disagreement relates.

10. If the individual has not submitted a written statement of disagreement, The University of Montana must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of protected health information only if the individual has requested such action.

11. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, The University of Montana must separately transmit the material required.

12. When the University of Montana is informed by another covered entity of an amendment to an individual's protected health information, The University of Montana must amend the protected health information in written or electronic form.

13. The University of Montana must document the titles for the persons or offices responsible for receiving and processing requests for amendments.

Additional Considerations of Amendments from Other Covered Entities

14. When a provider receives notification from another health care provider or health plan that a patient's protected health information has been amended, the receiving provider:

    a. Must ensure that the amendment is appended to the patient's health record; and
    b. Will inform its business associates that may use or rely on the patient's protected health information of the amendment (as agreed to in the business associate contract) so that they may make the necessary revisions based on the amendment.

Attachments to Policy

- ☐ Request for Amendment Form
- ☐ Sample Amendment Letters

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

REQUEST FOR AMENDMENT/CORRECTION OF PROTECTED HEALTH INFORMATION

Patient Name:	
Address:	
MR Account #:	
Birth Date:	
Request Date:	

WHAT NEEDS TO BE AMENDED/CORRECTED & WHY	
Entry to be Amended:	
Date & Author of Entry:	
Please Explain how the information is incorrect or incomplete. What should the information state to be more accurate or complete?	
Would you like this amendment sent to anyone whom we may have disclosed this information in the past? If so, please specify the name and address of the organization or individual.	
Name:	
Address:	
Name:	
Address:	

I understand that the provider may or may not amend the medical record with an amendment based on my request, and under no circumstances is the provider permitted to alter the original medical record. In any event, this request for an amendment will be made part of my permanent medical record.

_____ _____

Signature of Patient or Patient's Legal Representative Date

FOR HEALTH CARE ORGANIZATION/INTERNAL USE ONLY		
Date Received:	☐ Accepted	☐ Denied
If Denied, Check Reason for Denial:		
☐ PHI was not created by this organization	☐ PHI is not part of patient's designated record set	
☐ PHI is accurate and complete	☐ PHI is not available to the patient for inspection	
Comments: ☐ Individual was informed of denial in writing (attach letter of communication)		
_____ **Signature and Title of Staff Member**	_____ **Date**	

Mr. John A. Doe
123 Blank Street
Anytown, Montana 12345

January 1, 2012

Medical Record #: 123456
Filed: 00-00-00
Completed: 00-00-00

Dear Mr. Doe:

Thank you for submitting to us your "Request for Amendment/Correction of Health Information." Your request was forwarded to the _____ (*designated official*) for review.

Your request has been accepted, and the appropriate amendment has been made and added to your medical record. If you so indicated on your initial request, the amended information will be forwarded to the organizations or individuals you identified. If you did not indicate that we should forward the information, but would like us to do so, or if you would like us to forward the information to additional organizations or individuals, please contact (*contact name (or department), address, and phone number*).

Thank you for providing us with this opportunity to serve you and improve the accuracy and completeness of your health information. We look forward to continuing to serve your healthcare needs.

Sincerely,

Jane A. Doe, Privacy Officer
Anytown Community Hospital

SAMPLE LETTER **DENYING** INDIVIDUAL'S REQUEST FOR AMENDMENT OF HEALTH INFORMATION

Mr. John A. Doe
123 Blank Street
Anytown, Montana 12345

January 1, 2012

Medical Record #: 123456
Filed: 00-00-00
Completed: 00-00-00

Dear Mr. Doe:

Thank you for submitting to us your "Request for Amendment/Correction of Health Information." Your request was forwarded to the _____ (designated official) for review.

Your request has been denied for the following reason(s):

☐ The information was not created by this organization.
☐ The information is not available to you for inspection as permitted by federal law (e.g.,
☐ The information is not part of your designated record set.
☐ The information is accurate and complete.

If you disagree with this denial, you may file a written statement of disagreement with the (define appropriate organizational contact/office here). Please limit your statement to one typewritten page or two handwritten pages. If you choose not to file a statement of disagreement, you may request that we include your Request for Amendment/Correction of Health Information, as well as this denial of your request, with any future disclosures of the protected health information that is the subject of the requested amendment.

If you feel that you would like to file a complaint with the Secretary of the federal Department of Health and Human Services, you can address your complaint to 200 Independence Avenue, S.W.; Washington, DC 20201, or reach the Secretary by phone at (202) 690-7000.

Sincerely,

Jane A. Doe, Privacy Officer
Anytown Community Hospital

SAMPLE LETTER **RESPONDING** TO INDIVIDUAL'S STATEMENT OF DISAGREEMENT FOR DENIAL OF AMENDMENT OF HEALTH INFORMATION

Mr. John A. Doe
123 Blank Street
Anytown, Montana 12345

January 1, 2012

Medical Record #: 123456
Filed: 00-00-00
Completed: 00-00-00

Dear Mr. Doe:

We received your "Statement of Disagreement" in response to our letter notifying you that we denied your "Request for Amendment/Correction of Health Information." As part of the amendment request procedure, your initial request, your statement of disagreement, and supporting documents were forwarded for further review to a third party within our organization, who was not involved in the original decision to deny your request.

After considering your initial request, our denial of the request, and your statement of disagreement, along with your medical record, the third party determined that:

- ☐ The initial "Request for Amendment/Correction of Health Information" that you submitted will be honored and the requested amendment will be made.

- ☐ Your request continues to be denied. Your request for amendment, our denial of the request, your statement of disagreement, and our rebuttal statement, will be added to your medical record and will be included with any future disclosures regarding that information. (Please note that a "rebuttal statement" is not required. If our organization prepared one, it is enclosed with this letter.)

If you feel that you would like to file a complaint with the Secretary of the federal Department of Health and Human Services, you can address your complaint to 200 Independence Avenue, S.W.; Washington, DC 20201, or reach the Secretary by phone at (202) 690-7000.

Sincerely,

Jane A. Doe, Privacy Officer
Anytown Community Hospital

SAMPLE LETTER **NOTIFYING** INDIVIDUAL OF NEED FOR A 30-DAY EXTENSION IN RESPONDING TO REQUEST FOR AMENDMENT OF HEALTH INFORMATION

Mr. John A. Doe
123 Blank Street
Anytown, Montana 12345

January 1, 2012

Medical Record #: 123456
Filed: 00-00-00
Completed: 00-00-00

Dear Mr. Doe:

Thank you for submitting to us your "Request for Amendment/Correction of Health Information." Your request has been forwarded to the _____ (*designated official*) for review.

At this time, we are notifying you of the need for a 30-day extension in processing your request for amendment. This extension is necessary for the following reason(s):

(Insert Explanation/Reason for Extension)

We will notify you of our decision with regard to your request within the next 30 days.

Thank you for providing us with this opportunity to serve you and improve the accuracy and completeness of your health information. We look forward to continuing to serve your healthcare needs.

Sincerely,

Jane A. Doe, Privacy Officer
Anytown Community Hospital

PATIENT'S RIGHT TO REQUEST RESTRICTIONS ON CONFIDENTIAL COMMUNICATIONS

Policy

Patients/Individuals have the right to request restrictions on how and where their protected health information (PHI) is communicated. To comply with HIPAA Privacy Rule sections 164.502 and 164.522(b) regarding confidential communications, The University of Montana must permit patients/individuals to request to receive communications of PHI by alternative means or at alternative locations.

Procedures

1. The University of Montana may require that patient/individual requests to receive communications of PHI by alternative means or at alternative locations be made in writing. Writing requirements are detailed in the Notice of Privacy Practices.

2. Patients/Individuals may request to receive communications of PHI by alternative means or at alternative locations at the time of admission, visit, or at any time during the course of their care.

3. Patient/Individual requests may be made to any staff member of The University of Montana (e.g. Curry Health Center).

4. When patients/individuals make a request, either formally or informally, the staff member receiving the request should document it in writing.

5. The University of Montana must accommodate patient/individual requests that are reasonable.

6. The University of Montana must accommodate patient/individual requests that are reasonable, if the patient/individual states that the disclosure of PHI could endanger him or her.

7. The University of Montana determines whether a request is reasonable based solely on the administrative difficulty of accommodating the request. The University of Montana should establish policies and procedures to determine whether a request is reasonable.

8. The University of Montana may not require that patients/individuals provide a reason for their request.

9. The University of Montana may require that requests contain a statement that disclosure

of PHI could endanger the patient/individual. (The statement could be oral or written. Staff could ask patients/individuals if disclosure of PHI could put them in danger, or patients/individuals could fill out a request form that contains a checkbox question about possible endangerment due to PHI disclosure.)

10. The University of Montana may not deny requests based on its perception of whether patients/individuals have a good reason for making the request. A patient's/individual's reason for making a request cannot be used to determine whether the request is reasonable.

11. The University of Montana may deny patient/individual requests if:

    a. The patient/individual does not specify an alternative address or other method of contact.

    b. The patient/individual does not provide information as to how payment, if applicable, will be handled.

12. If The University of Montana grants a patient's/individual's request, the decision must be documented by maintaining a written or electronic record of the action taken.

13. If The University of Montana grants a patient's/individual's request, it provides appropriate staff with the communication requirements and requires staff to adhere to them.

PATIENT'S RIGHT TO REVOKE AUTHORIZATION FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION

Policy

An individual may revoke authorization at any time, provided the revocation is in writing, unless The University of Montana has already provided PHI based on the individual's authorization. The University of Montana will stop providing information based on the individual's authorization as soon as possible.

All supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process.

Procedure

The University of Montana's *Authorization For Disclosure of PHI* form shall give notice to individuals of their right to revoke an authorization of disclosure and the contact information of the person/office an individual is to contact in order to revoke authorization.

Attachment

Revocation of Authorization Form

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

REVOCATION OF AUTHORIZATION TO RELEASE INFORMATION

I, _____*(name)*, hereby revoke the authorization to release information I provided to {insert entity's name here} that allowed _____*(entity)* to use and disclose my Personal Health Information as I outlined on the Authorization Form, which I signed on _____*(Date)* for the release of my Personal Health Information to _____*(facility/person)*.

I understand that this revocation does not apply to any action _____*(entity)* has taken in reliance on the authorization I have previously signed. This revocation does not revoke any and all previous authorizations to release information that I have provided to _____*(entity)*.

_____ _____

Patient Name or Personal Representative *Date*

ACCOUNTING OF DISCLOSURES

Policy

This policy applies to all University of Montana covered entities to ensure that patients can receive an accounting of disclosures of their protected health information, not including disclosures for purposes of treatment, payment or health care operations. Disclosures to business partners must be included in the accounting. Under the Health Insurance Portability and Accountability Act, The University of Montana must give patients an accounting of disclosures, if requested. Patients may request an accounting of disclosures that were made up to six years prior to the date of request.

Procedures

1. Maintain an accounting of disclosures of protected health information on each patient for at least six years.

2. Information that must be maintained (tracked) and included in an accounting:

    A. Date of disclosure.
    B. Name of individual or entity who received the information and their address, if known.
    C. Brief description of the protected health information disclosed.
    D. Brief statement of the purpose of the disclosure or a copy of the individual's written authorization or a copy of the individual's written request for disclosure.
    E. Multiple disclosures to the same party for a single purpose or pursuant to a single authorization may have a summary entry. A summary entry includes all information (2 A-E) for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.

3. Information that is excluded from the accounting and tracking rule are disclosures made:

    A. Prior to April 14, 2003 or prior to the entity's date of compliance with the privacy standards.
    B. To law enforcement or correctional institutions as provided in state law.
    C. For listed information for facility directories.
    D. To the individual patient.
    E. To people involved in the patient's care.
    F. For treatment, payment, and healthcare operations.
    G. Pursuant to an individual's authorization.

4. All other disclosures of protected health information must be tracked. Disclosures are not limited to hard-copy information but any manner that divulges information, including verbal or electronic data release.

5. Disclosures may be tracked by a variety of internal processes that ensure accurate and complete accounting of disclosures.

    A. Computerized tracking systems that have the ability to sort by individual and/or date.
    B. Manual logs with one log per patient maintained in the patient's health record *(see sample "Disclosure Log" attached to this policy).*
    C. Authorization forms maintained in the patient's health record.

6. All systems must be maintained and accessible for a period of at least six years to meet the requirement of providing an accounting of disclosures for that time period.

7. Disclosures that are not accompanied by an authorization or a written request must be tracked by alternative computerized or hard-copy mechanisms.

8. A patient may make the request for an accounting in writing or orally. If the request is made orally, the organization should document such on the general "Authorization" form or a "Request for an Accounting of Disclosures" form *(see sample "Request of Accounting of Disclosures" form attached to this policy).* The organization must retain this request and a copy of the written accounting that was provided to the patient, as well as the name/departments responsible for the completion of the accounting.

9. A patient may authorize in writing that the accounting of disclosures be released to another individual or entity. The request must clearly identify all information required to carry out the request (name, address, phone number, etc.).

10. Provide the individual with an accounting of disclosures within 60 days after receipt of the request.

    A. If the accounting cannot be completed within 60 days after receipt of the request, provide the individual with a written statement of the reason for the delay and the expected completion date. Only one extension of time, 30 days maximum, per request is permitted.
    B. Requests can cover a period of up to six years prior to the date of the request.

11. Provide the accounting to the individual at no charge for a request made once during any twelve-month period. A reasonable fee can be charged for any additional requests made during a twelve month period provided that the individual is informed of the fee in advance and given an opportunity to withdraw or modify the request.

12. Maintain written requests for an accounting and written accountings provided to an individual for at least six years from the date it was created.

    A. Maintain the titles and names of the people responsible for receiving and processing accounting requests for a period of at least six years.

Attachments to Policy

- ☐ Request for an Accounting of Disclosures
- ☐ Disclosure Tracking Log

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

REQUEST FOR AN ACCOUNTING OF DISCLOSURES

PATIENT INFORMATION

Date of Request:	
Medical Record No.:	
Name:	
Date of Birth:	
Address:	
Address to Send Disclosure Accounting (If Different From Above):	

DATES REQUESTED

I would like an accounting of all disclosures for the following time frame. *Please note: the maximum time frame that can be requested is six years prior to the date of your request.*	
From Date:	
To Date:	

RESPONSE TIME

I understand the accounting I have requested will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.	
_____	
Signature of Patient or Legal Representative	**Date**

FOR HEALTH CARE ORGANIZATION USE ONLY	
Date Request Received:	
Date Accounting Sent:	Yes ☐ No ☐
Extension Requested:	
If Yes, Give a Reason:	
Patient Notified in Writing on This Date:	
Staff Member Processing Request:	

DISCLOSURE TRACKING LOG

Patient Name:	
Unit/MR#:	

KEY FOR TABLE

Auth Type:	How request was received
Purpose of Disclosure (PD):	**CC** = Continuing Care; **INS** = Insurance Processing; **LEG** = Legal Issue; Explain any other

Date Received	Name of Requestor	Address (If Known)	Auth Type	PD	PHI/Info Disclosed	Date Disclosed	Disclosed By:

(Use the above section as a complete record or to record those disclosures made w/o an authorization/written consent; complete fully if requested by patient/representative)

Requested By (Individual/Legal Rep)	Date Requested	Date Range Requested	Staff Member Completing Request	Date Provided

(Use the above section to document accounting requests when a copy of this disclosure log is provided to the individual requesting the accounting)

MANDATORY HIPAA EDUCATION AND TRAINING

Policy

All University of Montana students, faculty, employees, contract employees, and volunteers are required to attend and complete all applicable education, training and/or licensing courses as defined and required by the Montana University System and state and federal law.

Procedure

The University of Montana is responsible for providing the opportunity and direction needed to achieve the training and education required by this policy. The University of Montana must ensure that students and employees:

1. Comply with the institutional and departmental specific training and requirements; and

2. Attend and complete the training and have the attendance documented.

If a student/employee is unable to sufficiently complete the training requirement, it is the supervisor's obligation to ensure that the employee, student, etc. receives the proper guidance needed to fulfill the requirement.

PATIENT PRIVACY-RELATED COMPLAINTS

Policy

The University of Montana shall provide a process for a patient to file a complaint if the patient feels his or her privacy rights have been violated. The patient may also file a complaint concerning The University of Montana's privacy policies and procedures, even without alleging a violation of rights.

The University of Montana Chief Privacy Officer, Claudia Denker, is responsible for receiving complaints and shall establish a process for receiving, investigating and responding to patient complaints. She can be reached in the Office of Legal Counsel UH 132, 406-243-4755, Claudia.Eccles@umontana.edu. The patient complaint process is outlined in The University of Montana Notice of Privacy Practices. The University of Montana also recognizes the patient's right to file a complaint with the federal Department of Health and Human Services. The University of Montana shall cooperate with a federal investigation of the patient's complaint.

Any intimidation of or retaliation against patients, families, friends, or other participants in the complaint process is prohibited. Employees who violate this policy are subject to disciplinary action, up to and including termination.

If the patient's rights have been violated, employees who violated those rights are subject to disciplinary action, up to and including termination. The University of Montana shall mitigate, to the extent feasible, any known harmful effects of the violation.

Procedures

A. Filing a Complaint
   1. A patient may call, write, or present in person to the Compliance Officer or designated person the alleged privacy violation or complaint.
   2. The Compliance Officer or designated person will summarize the complaint on the Patient Complaint Report Form (attached).

B. Investigation of Complaint
   1. The Compliance Officer or designated person will facilitate the investigation of the complaint.

C. Response to Complaint
   1. A written response will be provided to the patient within 30 days from the date the complaint was filed.
   2. A written summary of the complaint and action taken will be filed with the Compliance Officer.

D. Translators, interpreters, and readers who meet the communication needs of the patient may be provided during the complaint process.

E. Patients are permitted to have a representative of their choice to represent their interests during the complaint process.

F. Occurrences representing potential liability claims will be referred to Risk Management.

G. Patients who request an outside agency to review their complaint may contact the Secretary of the federal Department of Health and Human Services at 200 Independence Avenue, S.W.; Washington, DC 20201, or reach the Secretary by phone at (202) 690-7000.

H. Documentation
   1. All complaints received must be documented.
   2. All complaint dispositions must be documented.
   3. The documentation must be retained for six years.

Attachments

Patient Complaint Report Form

UNIVERSITY OF MONTANA
A HYBRID ENTITY AS DEFINED BY HIPAA

PATIENT COMPLAINT REPORT FORM

Patient Name:	**Telephone:**
Address: _____	
_____	

Person Reporting (if other than patient above):		
Relationship to Patient:	**Telephone:**	
Address:		
Date Received:	**Time Received:**	**Received By:**
Report Received: ☐ In Person ☐ By Phone ☐ By Mail (Please Attach)		

Specifics of Report: _____

_____

_____

Summary of Investigation: _____

_____

_____

Response

Respondent:	**Date:**	**Time:**
Method of Response: ☐ In Person ☐ By Phone ☐ By Mail (Please Attach)		

Detail of Response (Attach if Written)**:** _____

_____

_____

SANCTIONS FOR FAILURE TO COMPLY WITH PRIVACY POLICIES

Policy

All employees are expected to acquaint themselves with performance criteria for their particular job and with all rules procedures, and standards of conduct established by the Board of Regents of the Montana University System and the employee's department or unit.

Any employee who does not fulfill the responsibilities set out by such performance criteria, rules, procedures, and standards of conduct may be subject to adverse disciplinary actions, as set forth below and in conjunction with the *Progressive Disciplinary Policy* of the Montana University System.

Sanctions applied vary depending on factors such as the severity of the violation, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information. Sanctions may range from a warning to termination.

Conduct Subject to Disciplinary Action

Work Performance: Failure of an employee to maintain satisfactory work performance standards constitutes good cause for disciplinary action which may include dismissal. The term Awork performance@ includes all aspects of an employee's work.

Misconduct: All employees are expected to maintain standards of conduct suitable and acceptable to the work environment. Disciplinary action, which may include dismissal, may be imposed for unacceptable conduct. Examples of unacceptable conduct, as applicable, include but are not limited to:

- Improper use or disclosure of an individual's Protected Health Information (PHI).
- Improper storage, copying, printing, and disposal of PHI.
- Creating or developing PHI documents that are greater than the minimum necessary for the specific task.

Types of Disciplinary Action

As set forth in the Montana University System's *Progressive Discipline Policy*, specific infractions shall be analyzed, and the appropriate penalty determined, on a case by case basis. All formal disciplinary actions shall be documented.

Types of disciplinary actions include but are not limited to written warnings, suspension without pay and discharge. Formal disciplinary actions may be combined or include other disciplinary measures such as a requirement to seek counseling, job transfer, demotion, cancellation of leave, last chance agreement, etc.

RETENTION OF RECORDS AND REASONABLE FEE FOR RELEASE

Policy

The University of Montana must retain the following records for the greater of six (6) years from the date of creation or last effective date of policies:

1. Authorization(s) documentation
2. Accountings of Disclosure (Copy of actual accounting and name of person/office providing authorization)
3. Person or Office responsible for processing requests for amendment and access
4. Record Sets available to individuals
5. Restrictions on use of disclosure agreed to by The University of Montana

The University of Montana may charge a reasonable fee to provide a copy of patient's health information. Fees may include only the cost of copying (supplies and labor), postage, and preparing a summary or explanation of an individual's PHI (if the individual agrees in advance to the summary and fees charged for preparation of such summary). The University may charge a reasonable fee, based upon actual costs, not exceeding 50 cents per page and $15.00 in administrative fees.

References

45 C.F.R. § 164.530(j)(2)
45 C.F.R. § 164.524(c)(4)
Mont. Code Ann. § 50-16-540

IDENTITY VERIFICATION

Policy

Obtain proper identification of all individuals, including patients, prior to allowing access to protected health information. Maintain patient confidentiality by obtaining identity verification of persons requesting the use and/or disclosure of protected health information as per the HIPAA standards, Section 164.512(h).

Procedures

1. Verify the identity of persons requesting any protected health information prior to allowing access to it.

2. Consult The University of Montana's Privacy Officer, Claudia Denker, in the Office of Legal Counsel, UH 132, 406-243-4755, Claudia.Eccles@umontana.edu before making any disclosure if uncertain whether or not sufficient verification has been obtained.

DESTRUCTION/DISPOSAL OF PATIENT HEALTH INFORMATION

Policy

It is the policy of The University of Montana to ensure the privacy and security of protected patient health information in the maintenance, retention, and eventual destruction/disposal of such media. Destruction/disposal of patient health information shall be carried out in accordance with federal and state law and as defined in the organizational retention policy. The schedule for destruction/disposal shall be suspended for records involved in any open investigation, audit, or litigation.

Patient Health Information Media

Any record of patient health information, regardless of medium or characteristic that can be retrieved at any time including all original patient records, documents, papers, letters, billing statements, x-rays, films, cards, photographs, sound and video recordings, microfilm, magnetic tape, electronic media, and other information recording media, regardless of physical form or characteristic, that are generated and/or received in connection with transacting patient care or business.

Procedures

1. All destruction/disposal of patient health information media will be done in accordance with federal and state law and pursuant to the organization's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed and disposed of in an appropriate manner.

2. Records involved in any open investigation, audit or litigation should not be destroyed or disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed and disposed of by the requesting party.

3. Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of patient information is complete.

4. A contract between the organization and a business associate must provide that, upon termination of the contract, the business associate will return or destroy and dispose of all patient health information. If such return or destruction/disposal is not feasible, the contract must limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal. These requirements also apply to a health plan that discloses patient health information to the plan sponsor.

5. A record of all patient health information media destruction/disposal should be made and retained permanently by the organization. Permanent retention is required because the records of destruction/disposal may become necessary to demonstrate that the patient information records were destroyed and disposed of in the regular course of business. Records of destruction/disposal should include:

    A. Date of destruction/disposal.
    B. Method of destruction/disposal.
    C. Description of the destroyed and disposed record series or medium.
    D. Inclusive dates covered.
    E. A statement that the patient information records were destroyed and disposed of in the normal course of business.
    F. The signatures of the individuals supervising and witnessing the destruction/disposal.

6. If destruction/disposal services are contracted, the contract must provide that the organization's business associate will

establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (outlined in the Business Associate Agreement Contract) and include the following elements:

A. Specify the method of destruction/disposal.
B. Specify the time that will elapse between acquisition and destruction/disposal of data media.
C. Establish safeguards against breaches in confidentiality.
D. Indemnify the organization from loss due to unauthorized disclosure.
E. Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.
F. Provide proof of destruction/disposal.

7. Patient information media should be destroyed and disposed of using a method that ensures the patient information cannot be recovered or reconstructed. Appropriate methods for destroying and disposing of media are outlined in the following table.

Medium	Recommendation
Audiotapes	Methods for destroying and disposing of audiotapes include recycling (tape over) or pulverizing.
Computerized Data/ Hard Disk Drives	Methods of destruction/disposal should destroy data permanently and irreversibly. Methods may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten. Total data destruction does not occur until the back-up tapes have been overwritten.
Computer Data/ Magnetic Media	Methods may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the back-up tapes have been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable.
Computer Diskettes	Methods for destroying and disposing of diskettes include reformatting, pulverizing, or magnetic degaussing.
Laser Disks	Disks used in "write once-read many" (WORM) document imaging cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/ Microfiche	Methods for destroying/disposing of microfilm or microfiche include recycling and pulverizing.
PHI Labeled Devices, Containers, Equipment, Etc.	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing labels or incineration of the medium would be appropriate.
Paper Records	Paper records should be destroyed and disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying and disposing of paper records include: burning, shredding, pulping, and pulverizing.
Videotapes	Methods for destroying and disposing of videotapes include recycling (tape over) or pulverizing.

8. The methods of destruction/disposal should be reassessed annually, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

Preservation or Destruction/Disposal of Patient Health Records Upon Closure of a Provider Office/Practice

9. The provider, or the provider's successor, shall comply with state law to ensure appropriate preservation, patient notice, and/or destruction/disposal of the patient health care records in the possession of the health care provider at the time the practice was ceased or the provider died. This statute does not apply to:

    A. Community-based residential facilities or nursing homes
    B. Hospitals
    C. Hospices
    D. Home Health Agencies

Attachments

Certificate of Destruction

CERTIFICATE OF DESTRUCTION

The information described below was destroyed in the normal course of business pursuant to the organizational retention schedule and destruction policies and procedures.

Date of Destruction:	**Authorized By:**

Description of Information Disposed Of/Destroyed:

Inclusive Dates Covered:

METHOD OF DESTRUCTION:

- ☐ Burning
- ☐ Overwriting
- ☐ Pulping
- ☐ Pulverizing
- ☐ Reformatting
- ☐ Shredding
- ☐ Other:

Records Destroyed By*:

If On Site, Witnessed By:

Department Manager:

**If records destroyed by outside firm, must confirm a contract exists*