POLICY

Subject: Health Insurance Portability and Accountability Act (HIPAA): Flexible Benefits HIPAA Privacy Policy

The Colorado School of Mines ("CSM") is the plan sponsor for the faculty Flexible Benefits Program. The plan is administered by PayFlex, through a Business Associate relationship. Certain employees of CSM or of PayFlex may have access to the individually identifiable health information (as defined by HIPAA) of participants in the Flexible Spending Account for Health Care Expenses ("FSA") in order to administer the program.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations restrict the Plan's ability to use and disclose protected health information for administration of the plan:

Protected Health Information ("PHI).

For purposes of the FSA and CSM's use, including CSM's employees, PHI generally means information that is created or received by the Flexible Benefits Program and is related to enrollment, contributions or payments.

While CSM employees do not have access to the following, PayFlex and its employees may have access to and use the PHI described below in addition to the enrollment, contributions and payments information in order to administer the FSA. Examples of additional PHI under HIPAA may include: the past, present, or future physical or mental health or condition of a participant, or the past, present, or future payment for the provision of health care to a participant and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

It is CSM's policy to comply fully with HIPAA's requirements. To that end, all members of the CSM workforce who have access to PHI related to the FSA must comply with this Privacy Policy and Procedures. For purposes of this Policy and Procedures, the CSM Flexible Benefits Program workforce includes the Associate Vice President of Human Resources, the Assistant Director, the Benefits Manager, the Benefits Technician, the HR Data Technician, all Payroll Office employees, and Information Services employees who support the HRS/Payroll system. Additionally, all Business Associates and their employees must also comply with HIPAA, this Policy and Procedures, and their Business Associate contract.

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

HIPAA PRIVACY PROCEDURES

Use and Disclosure of PHI

I. Use and Disclosure Defined

The CSM Flexible Benefits Program will use and disclose PHI only as permitted under HIPAA for treatment, payment, operations and certain public policy disclosures. The terms "use" and "disclosure" are defined as follows:

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

II. Workforce Must Comply With Plan's Policy and Procedures

All members of the CSM Flexible Benefits Program workforce (described at the beginning of this Policy and referred to herein as "Employees") must comply with this Policy and Procedures.

III. Access to PHI is Limited to Certain Employees

The following Employees ("employees with access") have access to PHI:

- Associate Vice President of Human Resources who performs functions directly on behalf of the program and the Assistant Director of Human Resources on behalf of the Associate Vice President of Human Resources.
- Benefits Manager who perform administrative and participant services directly within the program;
- HR Data Technician and the Benefits Technician who have access to PHI on behalf of the program for use in administrative functions (e.g., enrollments, benefits selection data entry, billing reconciliation);
- Payroll Office staff who access participation, contribution levels, billing reconciliation and payments to Business Associates; and
- Information Services staff who support the HRS/Payroll system and who may access data in their role of programming, troubleshooting systems problems, or performing security operations or audits.

Employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other Employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan

administrative function). Employees with access may not disclose PHI to other persons (other than Employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and Procedures.

IV. Specific Uses and Disclosures

A. Treatment, Payment and Health Care Operations

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

- *Payment*. Payment includes activities undertaken to obtain program contributions or to determine or fulfill the program's responsibility for provision of benefits under the FSA.

PHI may be disclosed for purposes of the Flexible Benefits Program's own ***health care operations***.

- *Health Care Operations*. Health care operations means any of the following activities to the extent that they are related to Plan administration:
  Enrollments and enrollment changes.
  Conducting or arranging for legal services and auditing functions.
  Claims processing.
  Billing

- **Treatment. PHI may be disclosed to a health care provider if necessary for treatment.**

B. For Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operation of CSM's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.) unless the participant has provided an authorization form for such use or disclosure, or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

C. To Individual and the U. S. Department of Health and Human Services

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

- The disclosure is to the individual who is the subject of the information.
- The disclosure is made to the U. S. Department of Health and Human Services ("HHS") for purposes of enforcing HIPAA.

D. For Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. These requirements include prior approval of the CSM Privacy Official. Disclosures without authorization are permitted:

- about victims of abuse, neglect or domestic violence;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents; and
- for specialized government functions.

E. Pursuant to an Authorization

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

F. To Spouses, Family Members, and Friends

CSM Employees will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI. If an Employee receives a request for disclosure of an individual's PHI from a spouse, family member or personal friend of an individual, and the spouse, family member, or personal friend who is the personal representative of the individual, the procedure for "Verification of Identity of Those Requesting Protected Health Information" will be followed (see Section VII below).

G. To Business Associates

Business Associate is an entity or person who:

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

    - The third party administrator retained to administer the CSM Flexible Benefits Program is a business associate to the Program.

Employees may disclose PHI to the Plan's Business Associates and allow the Plan's Business Associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the Business Associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "Business Associate," Employees must contact the Privacy Official and verify that a Business Associate contract is in place. Disclosures must be consistent with the terms of the Business Associate contract.

H. De-Identified Information

The Plan may use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Employees will obtain approval from Privacy Official for the disclosure. The Privacy Official will verify that the information is de-identified.

V. Minimum Necessary Standard and Disclosures

The "minimum necessary" standard applies to disclosures described in IV(A), IV(B), IV(D), and IV(G). This standard generally requires that when PHI is used or disclosed, the amount of information disclosed must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

Procedures for Disclosures and Requests for Protected Health Information
For recurring disclosures and requests (e.g., to business associates), and all other disclosures and requests, the Privacy Official will be consulted to ensure that the amount of information disclosed is the minimum amount necessary to accomplish the purpose of the request or disclosure.

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

- Uses or disclosures made to the individual.
- Uses or disclosures made pursuant to an individual authorization.
- Disclosures made to U. S. Department of Health and Human Services.
- Uses or disclosures required by law
- Uses or disclosures required to comply with HIPA and
- Uses or disclosures to a provider for treatment.

VI. Privacy Official Approval of Disclosures

Requests for disclosures described in IV(B), IV(D), and IV(F) shall be submitted in writing to the Privacy Official who will determine the appropriateness of the request based on applicable regulations, and if necessary, consultation with the Plan's legal counsel.

VII. Verification of Identity of Those Requesting Protected Health Information

Verifying Identity and Authority of Requesting Party. Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a spouse, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access.

Request Made by Individual. When an individual requests access to his or her own PHI, the following steps should be followed.

- Unless the individual is personally known to the Employee, request a form of identification from the individual. Employees may rely on a valid driver's license, student or faculty ID, passport or other photo identification issued by a government agency.
- Make a copy of the identification provided by the individual and file it with the request.
- If the individual requests PHI over the telephone, the Employee will ask for the individual's subscriber identification number and home address for verification; however, if the Employee is not sure of the identity of the caller, the Employee will advise the caller that he or she must make the request in person.

Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:

- Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.

Request Made by a Spouse or by a Personal Representative. When a spouse or a personal representative requests access to an individual's PHI, the following steps should be followed:

- Require a copy of a valid power of attorney or appointment of personal representative.
- Make a copy of the documentation provided and file it with the individual's request.

Who Must Be Recognized as the Individual's Personal Representative. The following chart displays who must be recognized as the personal representative for a category of individuals:

If the Individual Is:	The Personal Representative Is:
An Adult or Emancipated Minor	A person with legal authority to make An health care decisions on behalf of the Individual *Examples*: Health care power of attorney Court appointed legal guardian
An Unemancipated Minor	A parent, guardian, or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor child *Exceptions*: See parents and minors discussion below.
Deceased	A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions)

Request Made by Public Official. If a public official requests access to PHI, and if the request is for one of the purposes set forth above in IV(C) or IV(D), the following steps should be followed to verify the official's identity and authority:

- If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's request and records.
- If the request is in writing, verify that the request is on the appropriate government letterhead and contact the requesting agency to verify the request;
- Obtain approval for the disclosure from the Privacy Official.

Questions about validity or authorization.
Verify that the identification matches the identity of the individual requesting access to the PHI. If the Employee has any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.

Complying with Individual Rights

I. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their own PHI that the Plan or its Business Associates maintain in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The CSM Flexible Benefits Program will provide access to PHI and will consider requests for amendment that are submitted in writing by participants.

Designated Record Set is a group of records maintained by or for the FSA that includes:

- The enrollment, payment, and claims adjudication record of an individual maintained by or for the program; or
- Other PHI used, in whole or in part, by or for the FSA to make coverage decisions about an individual.

Procedure

- Follow the procedures for verifying the identity of the individual (or spouse, parent or personal representative) set forth in the ""Verification of Identity of Those Requesting PHI."
- Review the disclosure request to determine whether the PHI requested is held in the individual's designated record set. No request for access may be denied without approval from the Privacy Official.
- Respond to the request by providing the information or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days with written notice to the individual outlining the reasons for the extension and the date by which the Plan will respond.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made since April 14, 2004, (but not farther back in time than the previous six years if April 14, 2004, is more than six years from the date of the request), **other** than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- as part of a limited data set; or
- for national security or law enforcement purposes.

Procedure

- The Privacy Official will respond to the request within 60 days by providing the accounting or informing the individual that there have been no disclosures that must be included in an accounting. If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days with written notice to the individual outlining the reasons for the extension and the date by which the Plan will respond.
- If any Business Associate of the Plan has the authority to disclose the individual's PHI, then CSM Flexible Benefits Program Employees will submit the individual's written request.
- Accountings must be documented in accordance with the procedure for "Documentation Requirements."

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the CSM Flexible Benefits Program, the requests are reasonable. CSM Flexible Benefits Program Employees shall accommodate such a request if the participant clearly provides information that the disclosures of all or part of that information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications. See Appendix for "Participant Request for Confidential Communication" form for such requests.

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

A participant may request restrictions on the use and disclosure of the participant's PHI. It is CSM's policy to attempt to honor such requests, if, in the sole discretion of the CSM Flexible Benefits Program, the requests are reasonable.

V. Request for Amendment

A participant may request the CSM Flexible Benefits Program to amend PHI. The CSM Flexible Benefits Program is not required to delete, amend or expunge any PHI from their

records under the HIPAA privacy rules. You must submit a written request to the Privacy Official to amend your PHI maintained by the CSM Flexible Benefits Program in its designated record set. The Privacy Official will make a decision on the request to amend within 60 days of receiving your request or advise you that an additional 30 days is needed to review your request. If the CSM Program does not agree to amend the PHI, it will notify you in writing and explain the reason for the denial. You may submit a written statement of disagreement on the decision to the Privacy Official.

Other Procedures

Privacy Official and Contact Person

The CSM Benefits Manager will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and Procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

Workforce Training

CSM will train all Employees on its Privacy policy and Procedures. The Privacy Official is charged with developing training programs so that Employees receive the training necessary and appropriate to permit them to carry out their functions within the Flexible Benefits Program.

Technical and Physical Safeguards

The CSM Flexible Benefits Program will establish appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Physical safeguards include locking doors and filing cabinets.

Privacy Notice

The Privacy Official is responsible for maintaining and issuing a notice of the CSM Flexible Benefits Program privacy practices. The privacy notice will inform participants that the CSM Flexible Benefits Program will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the Plan's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually electronically delivered to all participants unless a participant requests delivery of a printed copy. In this instance, the participant will be provided a printed copy. The CSM Flexible Benefits Program will also provide notice of availability of the privacy notice at least once every three years.

Documentation Requirement

The CSM Flexible Benefits Program Employees will document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

Documentation. The CSM Flexible Benefits Program will maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued to participants.
- When a disclosure of PHI that requires accounting is made:
  - the date of the disclosure;
  - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - a brief description of the PHI disclosed; and
  - any other documentation required under these Use and Disclosure Policy and Procedures.
- Individual Authorizations.
- Requests for Amendments.
- Accounting of Disclosures.
- Requests for Restrictions on Uses and Disclosures of PHI.

Policies and procedures will be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes in policies or procedures will be promptly documented.

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

Plan Document

The Plan document shall include provisions to describe the permitted and required uses and disclosures of PHI by the CSM Flexible Benefits Plan for administrative purposes.

Complaints

The CSM Benefits Manager, 303.273.3528, will be the Plan's contact person for receiving complaints.

All complaints must be in writing and include the date of the complaint, the date of the alleged violation, the name of the party against whom the complaint is made, the substance of the complaint and the name and signature of the complainant. The Privacy Official will investigate the complaint, question the individual making the complaint if necessary, question the party alleged to have violated the Privacy Policy and consider any documents, evidence or testimony related to the incident. The Privacy Official will make a determination

on whether there has been a violation of CSM Privacy Policy within 60 days of receiving the written complaint. The Privacy Official will determine whether any corrective action is necessary and implement any corrective measures. When appropriate the Privacy Official will inform the employee of the determination made with regard to the complaint. The Privacy Official will document and keep a record of the complaint and investigation for a six year period.

The Privacy Official is responsible for providing a process for individuals to lodge complaints about the CSM Flexible Benefits Program's Privacy Policy and Procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this Privacy Policy and Procedures will be imposed in accordance with applicable law and policies, up to and including termination. The Privacy Official will document any sanction imposed for violation of this Privacy Policy.

No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

CSM and its employees may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

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

X. Mitigation of Inadvertent Disclosures of Protected Health Information

HIPAA requires that the CSM Flexible Benefits Plan mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual's PHI in violation of this Policy and Procedures. As a result, if the CSM Flexible Benefits Program Employees or plan participants become aware of a disclosure of PHI, either by an Employee of the CSM Flexible Benefits Program Office or an outside consultant/contractor, that is not in compliance with this Policy and Procedures, the Employee or participant should immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the individual can be taken.

*****COLORADO SCHOOL OF MINES NOTICE OF PRIVACY PRACTICES*****
Effective Date: March 19, 2008

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.

Why have you been sent this Notice?
The Colorado School of Mines (CSM) Flexible Benefit Program is required under the Privacy Regulations of the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d – 1320d-8, and its implementing regulations, 45 C.F.R. Parts 160 and 164, (HIPAA) to provide all employees eligible to participate in the Program with this notice of privacy practices. This notice concerns the personal, protected health information (PHI) you have provided to the Program and any third party administrators in connection with the flexible spending account provisions of the Program. CSM takes your privacy seriously. Your information will not be used or disclosed without your written authorization, except as described in this notice or as otherwise permitted by Federal and State law. You may revoke your authorization as provided by the HIPAA Privacy Regulations.

How do we use your information?
We restrict access to your PHI to those employees of CSM who need to know the information in order to provide services to you. CSM uses your PHI without your written authorization for purposes of treatment, payment, or health care operations, which are explained below:

- Treatment is health care. For example, the Program may disclose PHI and confirm your program eligibility so that treatment is provided to you.
- Payment is paying claims for health care and related activities. For example, the Program may disclose your PHI to adjudicate claims and appeals.
- Health Care Operations is the administration and operation of the program. For example, the Program may disclose your PHI to evaluate the quality of service that you receive.

With whom do we share your information? CSM may share your PHI, without your written authorization, with the vendors that assist CSM in providing services to you for the Program. If we share your information, the vendors have an obligation not to disclose or use your information for any other purpose, except as permitted by HIPAA and other law.

When else do we use or share your information?
There are limited circumstances when CSM is permitted or required to use or disclose your PHI without your written authorization. These situations include:

- to keep you informed of health related benefits or services that may be of interest to you,
- public health purposes,
- medical emergencies,
- use by medical examiners, coroners, funeral directors and organ donation organizations,
- judicial and administrative proceedings and law enforcement purposes,
- specialized government functions, such as military, intelligence and correctional activities,
- when otherwise required or permitted by law.

What are our duties?
CSM is required by law to:

- maintain the privacy of your PHI,
- provide this notice of our duties and privacy practices with respect to PHI,
- follow the procedures described in this notice,
- inform you that it reserves the right to change its privacy practices and the terms of this notice and to make the new notice provisions effective for all PHI. Revised notices will be made available to you by posting on our website and notifying you through campus e-mail.

What are your rights?
You have the right to:

- request that CSM restrict how it uses/discloses your PHI, CSM will consider your request but is not legally required to agree
- request that CSM communicate your PHI to you via alternative means or at alternate locations,
- inspect and copy your PHI (fees may apply),
- request additions or corrections to your PHI, CSM will consider your request but is not legally required to agree to it,
- receive an accounting of disclosures of your PHI made by CSM for reasons other than treatment, payment, health care operations and disclosures to you or authorized by you,
- obtain a paper copy of this notice upon request,
- complain to CSM and to the Secretary of Health and Human Services in Washington D.C. if you believe your privacy rights have been violated.

To contact us:
If you would like to exercise your rights, or if you feel that your privacy rights have been violated or if you need more information, you may write to the Privacy Officer at the following address: Colorado School of Mines, Attn: Human Resources, 1500 Illinois Street, Golden, CO, 80401 or call (303) 273-3250.

All complaints will be investigated and you will not be retaliated against for filing a complaint.

Appendices

Participant Information Amendment Form

I, _____ (Participant's name) request that information kept in the records of the Colorado School of Mines be amended.

Information to be Amended

Item to be changed:

Data source:

Change:

Reason:

If you need help with this form, please contact: **Colorado School of Mines Privacy Official, 303 273-3528**. *Attach additional copies of this page as needed.*

_____ _____
Signature of Participant or Personal Representative: Date

_____
Print Name of Participant or Personal Representative

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

_____
_____
_____

This section to be filled out by Privacy Official

Approved Amendments

The following requests for amendment of information have been

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

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

Participant Request for Confidential Communication

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

Designated Method of Contacting the Participant

Communications with the Participant named above should be directed to:

Mailing Name

Street Address

City, State & Zip

Telephone Number

Name of Participant: _____

Address of Participant: _____

_____

_____ _____

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

_____

Print Name of Participant or Personal Representative

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

_____

_____

_____

Acknowledgment of Receipt of Privacy Practices

I, _____ have received a copy of the Colorado School of Mines' Notice of Privacy Practices with an effective date of _____

Name of Participant: _____

Address of Participant _____

_____

_____ _____

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

_____

Print Name of Participant or Personal Representative

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

_____

_____

_____

Name of Witness _____

Signature of Witness _____ *Date* _____

Authorization Revocation Form

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

Effect of Revocation

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

Other consequences of revoking authorization include:

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

Name of Participant _____

Address of Participant _____

_____

_____ _____

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

_____

Print Name of Participant or Personal Representative

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

_____

_____

_____

Authorization for Use or Disclosure of Protected Health Information

I, _____, authorize the Colorado School of Mines Flexible Benefits Program and its employees to (check all that apply):

Θ use the following protected health information,

Θ disclose the following protected health information to:

_____
_____
_____
_____

Information to be used or disclosed.

_____

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

_____

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

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

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

Privacy Official, Colorado School of Mines, Human Resources, 1500 Illinois Street, Golden, Colorado 80401

I understand that if I decide at a future date to revoke this authorization, such a revocation is not effective to the extent that my health care provider has relied on the use or disclosure of the protected health information.The CSM Flexible Benefits Program may not condition treatment, payment enrollment or eligibility for benefit on whether I sign this authorization. I understand that I have a right to request a copy of this Authorization.

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

_____ _____

Signature of Participant or Personal Representative **Date**

_____

Print Name of Participant or Personal Representative

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

_____
_____
_____

COLORADO SCHOOL OF MINES
CONFIDENTIALITY AND INFORMATION SECURITY AGREEMENT

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

I ACKNOWLEDGE, UNDERSTAND, AND AGREE:

1. The types and categories of written, verbal, electronic or printed information that are considered to be confidential ("CONFIDENTIAL INFORMATION") includes, but is not limited to: (a) medical records; (b) medical records received from other health care providers; (c) correspondence addressed to or from employees of the CSM concerning a specific, identifiable participant; (d) participant information verbally given to me by the participant or other persons; (e) health spending account salary reductions; (f) demographic data; (g) financial/-funding information; (h) Social Security numbers; (i) protected health information held or created by the CSM Flexible Benefits Program, (j) payroll and benefit information on participants and employees, and (k) all other types and categories of information to which I know or have reason to know CSM intends or expects confidentiality to be maintained.

2. Services provided by CSM for its participants and all documents and information related to such services are private and CONFIDENTIAL INFORMATION.

3. Participants furnish information to CSM with the understanding and expectation that it will be kept confidential and used only by authorized persons, within the scope of their employment, as necessary, to provide needed services.

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

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

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

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

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

9. By reason of my duties or in the course of my employment, I may receive or have access to verbal, written or electronic information concerning participants. I will not inappropriately access, use, or disclose (verbally, in written form, or by electronic means) to any person, or permit any person to inappropriately access, use, or disclose any reports or other documents prepared by me, coming into my possession or control, or to which I have access, nor any other information concerning the participants or operations of the healthcare flexible spending account at any time, during or after my employment.

10. If and when my employment or assignment with CSM ends, I will not inappropriately access, use, disclose, retain, or copy any reports or other documents prepared by me, coming into my possession or control, or to which I have access, nor any other information concerning the participants or healthcare flexible spending account operations of the CSM.

11. I will not destroy or erase any participant or healthcare flexible spending account data or information in any form located in or stored in CSM computers or files unless it is part of routine computer maintenance.

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

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

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

15. I will maintain the confidentiality of all information concerning participants or healthcare flexible spending account operations of CSM regardless of the method of retrieval, including information obtained on home-based or off-site personal computers.

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

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

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

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

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

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

22. I may access my own Confidential Information via an electronic application, pursuant to established policies, but I may not access that of my spouse, children, family members, friends or co-workers without proper authorization.

23. I will not access data on participants for whom I have no responsibility or for whom I have no "need to know." Audit trails will track unauthorized access.

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

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

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

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

28. If I receive access to information stores such, as the IS's data warehouse, or other databases containing CONFIDENTIAL INFORMATION, I will use that access only for the intended and stated purpose and will not provide access to third parties without the explicit written permission of the IS's data steward. I will utilize data obtained from such information stores in conjunction with data use policies.

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

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

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

Employee Information

Name: _____
(Please Print)

Telephone #: _____

Title: _____

Assigned Unit/-CSM: _____

Today's Date: _____

Employee Signature: _____