Mountain State Blue Cross/Blue Shield

Health Insurance Portability and Accountability Act ("HIPAA")

Policies and Procedures Regarding Protection of the Privacy of Personal Health Information

Training Manual

Mountain State Blue Cross/Blue Shield

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ("HIPAA") POLICIES AND PROCEDURES REGARDING PROTECTION OF THE PRIVACY OF PERSONAL HEALTH INFORMATION

TABLE OF CONTENTS

Cross/Blue Shield

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ("HIPAA") POLICIES AND PROCEDURES REGARDING PROTECTION OF THE PRIVACY OF PERSONAL HEALTH INFORMATION

Training Manual

Mountain State Blue Cross/Blue Shield (the "Plan") has implemented a policy and procedures in order to protect and enforce the rights of the employees (and retirees, if applicable) who participate in the Plan, along with their covered spouses and dependents, to privacy in their Individually Identifiable Health Information and to fulfill the Plan's legal obligations under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), 42 U.S.C. Section 1302d, et seq., and regulations promulgated there under, collectively referred to as "HIPAA" or the "Privacy Regulations".

While the policy and procedures cover a substantial portion of the HIPAA requirements applicable to the Plan, they are not a comprehensive description of the law and should not he considered a substitute for reading the provisions of HIPAA or the advice of legal counsel, when advisable or necessary. In addition, specific state law provisions that may not be covered in the policy may contain requirements regarding the use or disclosure of a person's Health Information and may in certain instances exceed the requirements set forth in the HIPAA Privacy Regulations.

If you have any questions or concerns regarding this manual, the HIPAA privacy police and procedures, or your obligations under any of them or under state or federal law, please contact the Plan's Privacy Officer (the Director of Human Resources) at (304)829-7210 *or* by mail at P O Box 417, Bethany, WV 26032.

I. What Benefit Programs Are Subject To The Rules?

The HIPAA Privacy Regulations apply to three types of entities: Healthcare Providers. Healthcare clearinghouses and Group Health Plans. The definition of a "Group Health Plan" subject to the rules is very broad. It includes health maintenance organizations as well as any employee welfare benefit plan that provides medical care or services to employees and their dependents as long as the plan covers 50 or more participants or is administered by an entity other than the employer that sponsors the plan. Thus, the Plan is subject to the Privacy Regulations.

Healthcare is defined in broad enough terms that the rules apply not only to the medical coverage portion of the Plan, but also to any available dental, vision and mental health plans, prescription drug plans, healthier flexible spending accounts and similar benefits. Any other healthier plans or programs offered to employees on a pre-tax basis will also need to comply. While many of these benefit programs are administered by other parties, there still are circumstances when information will come into contact with someone at the company or one of its affiliated companies, if any, and need to be handled in accordance with these new privacy procedures. ***See Appendix A for a list of the benefit programs that must comply with the HIPAA Privacy Regulations.***

HIPAA does not cover other employee benefit programs even though such programs may have or use Health Information. Benefit programs such as accidental death and dismemberment insurance, short and long-term disability programs, life insurance, liability insurance, automobile medical

payment insurance, coverage for on-site medical clinics, workers' compensation and other similar insurance coverage where benefits for healthcare are secondary or incidental do not have to comply with the HIPAA privacy rules.

In addition, HIPAA does not protect Health Information that is obtained and used by the employer for employment purposes. For instance, information given to the employer as part of a pre-employment physical or in a request for a leave of absence under the Family and Medical Leave Act ("FMLA") is not covered or protected by HIPAA.

Common Questions and Answers:

Q1: What benefit programs are covered by the HIPAA Privacy Regulations?

A1: Generally, all of the medical, dental, vision, mental health and prescription drug programs of the Plan, the healthcare flexible spending account and the EAP are covered by the HIPAA Privacy Regulations. ***See Appendix A for a complete list.***

Q2: Our EAP only provides referrals; is it subject to the rules?

A2: Yes, it is. Although the EAP only provides referrals, it still maintains individually identifiable information pertaining to health benefits such as the individual's name, date of birth and eligibility for benefits under the plan.

Q3: **Is Health Information contained in our employment records subject to these rules?**

A3: No, information obtained by the employer for employment-related functions is not Protected Health Information or "PHI" under HIPAA *(see the Glossary at the end for definitions of key terms capitalized in this manual).* While this information should be maintained in separate files apart from the individual's personnel or employment records and the employer should use discretion and good judgment in using and sharing such information, the information is not PHI. Note, however, that if the employer wants to obtain Health Information from a provider instead of the employee, the Healthcare Provider may require a signed Authorization before releasing the information to the employer.

Q4: Our short-term/long-term disability vendor has requested information from the health plan. Can we provide the requested data?

A4: No. Although short-term and long-term disability programs are not subject to the HIPAA privacy rules, the health plan cannot share PHI with a non-covered entity without an Individual's Authorization. However, if the requested information can be De-identified or summarized in a Limited Data Set, the health plan could share the information with the STD/LTD vendor. *(See Section IX, for more details.)*

II. Overview Of Requirements.

The Privacy Regulations require the Plan to adopt and follow procedures that are intended to safeguard the privacy of an Individual's Protected Health Information, ensure that Business Associates of the Plan do likewise, and provide certain rights to Individuals with respect to their own PHI. There are rules regarding when PHI may be Used or Disclosed without an Individual's consent or Authorization, when such

an Authorization is required, and when. if identifying information is removed, Health Information is otherwise disclosable in summary or De-identified form. The Plan is also required to designate a Privacy Officer and a Complaint Officer. The Plan's Privacy Officer is responsible to oversee compliance. The Complaint Officer will receive and process any complaints that the rules have not been followed. Finally, the Plan must also disclose to covered employees what the Plan's privacy policy and procedures are, and advise them of their rights under the law. A notice covering the required disclosures must be given to employees covered under the Plan.

Generally, the Plan may Use or Disclose PHI for its own purposes of Payment or Healthcare Operations, as described in Section IV below, without first obtaining a Participant's Authorization or otherwise meeting an exception under the Regulations. Further, the Plan may Disclose PHI to a provider for that provider's Treatment purposes, or for another Covered Entity's or provider's Payment purposes, without an Authorization. Also, under certain circumstances, the Plan may Disclose PHI for limited Healthcare Operations of another Covered Entity, such as quality assessment and practitioner review or credentialing purposes, provided the other Covered Entity also has (or had) a relationship with the Participant.

Unless otherwise permitted or required by the Privacy Regulations, the Plan may not Use PHI obtained from any source or Disclose PHI maintained by or in the possession or control of the Plan, unless an Individual has provided his or her prior written Authorization approving such Use or Disclosure, either directly to the Plan or through a Healthcare Provider or other Covered Entity. The Plan's Authorization forms must comply with the specific content requirements set forth by the Privacy Regulations. The Plan must permit an Individual to request in the Authorization that restrictions be placed on the Plan's Use and Disclosure of that Individuals PHI. The Plan will seriously consider each such requested restriction; however, the Plan is not required to accept an Individual's requested restrictions. If the Plan does accept an Individual's requested restriction, the Plan is bound to abide by those restrictions. The Plan generally may not condition enrollment or eligibility on the Participant's or other covered dependent's (together referred to as "Participant") provision of an Authorization. However, the Plan may condition enrollment in the Plan or eligibility for benefits prior to enrollment or giving an Authorization if the Authorization sought is for the Plan's own eligibility or enrollment determinations or underwriting or risk rating determinations. A Participant may revoke an Authorization at any time by providing written notice of revocation to the Plan. The Plan may not rely on an Authorization that it knows has been revoked. In addition, some special rules apply to the Use and Disclosure of Psychotherapy Notes.

Common Questions and ***Answers:***

Q1: Will we have to administer our benefit programs differently?

A1: Yes, to some extent. PHI created or received by the "Group Health Plan" (those programs under the Plan that are subject to the HIPAA Privacy Regulations) may not be shared with other benefit programs, such as the long-term disability program, without an Authorization from the Participant. Even with an Authorization, only the Minimum Necessary amount of PHI may be Used or Disclosed to meet the stated reason for the Disclosure. For example. if an employee is applying for long-term disability ("LTD") benefits, information acquired about his or her condition through the health plan's payment of claims cannot be shared with the LTD carrier unless the employee Authorizes it in writing.

Q2: Is information concerning enrollment or participation status in the group health programs PHI?

A2: Yes, it is. However, there is an exception in the HIPAA Privacy Regulations that permits the Plan to share enrollment and disenrollment information with the Plan's Sponsor (the company) without requiring an Individual's Authorization. This enables the company to communicate with the Plan and its Business Associates about who is eligible for coverage under the plan.

Q3. A hospital emergency room calls to verify that a newly admitted patient is covered by our plan; can we still answer that question?

A3: Yes. The reason for the inquiry is for Payment and possible Treatment purposes and is a permissible Disclosure of PHI.

Q4: A new employee's former employer calls to see if the employee is eligible for our health plan so that the former employer can terminate COBRA coverage. Can we tell them if the employee is enrolled?

A4: No. You must have an Authorization from the employee before you can Disclose this information.

III. Who Has Access To PHI?

In most cases, it will be the actual Healthcare Providers, such as doctors and hospitals. who hold and have access to PHI. The Plan may not actually possess PHI, but will have access to PHI through the Plan's association with its Business Associates. those entities providing services to the Plan. In addition, company employees who assist in the administration of Plan activities may also have access to PHI from time to time in order to complete their Plan administrative duties. For example, human resources employees may request and Use PHI in order to assist a Participant with a claims issue, to answer eligibility questions or to assist with an appeal of a denied claim through the Plan's claims appeal process. Employees who need to have access to PHI must be identified by the Plan and be trained in the Privacy Regulations and the Plan's HIPAA privacy policy and procedures. The human resources employees and others who may encounter PHI while performing their Plan administration functions are referred to as the Plan's "Workforce".

Individuals who are not members of the Plan's Workforce, such as other company supervisors or employees, and individuals representing an outside entity that is not a Business Associate of the Plan, may not have access to PHI unless the Disclosure is permitted under the Privacy Regulations or the information is provided pursuant to a Participant's Authorization to release the PHI.

Common Questions and Answers:

Q1: What are "Plan administration functions"?

AI: Many if not most Plan administration functions are outsourced to various vendors or Business Associates. Examples of Plan administration functions that may he handled by company employees include answering eligibility questions, assisting an employee with a claims payment question, enrolling new employees into the Plan, presenting a claims appeal for consideration and reviewing an explanation of benefits (or "EOB") with an employee. Also, see the definitions of Payment and Healthcare Operations in Section IV below for additional information.

Q2: Who is the Plan's "Workforce"?

A2: The Plan's Workforce includes those human resources employees and other company employees who are responsible for any of the day-to-day activities and administrative duties of the Plan. If you have any questions about Plan administration issues or are not certain who should handle it, call the Human Resource Department.

Q3: The company is my employer, not the Plan. How can I tell if I'm working for the Plan?

A3: It is very common for employees to "wear" multiple hats because they have responsibility for a number of different human resource or company functions. Employees in this situation must be aware of when they are acting on behalf of the Plan and when they are performing other functions, even if they may be using some of the same information. If you are engaged in an activity that primarily assists the company, such as deciding whether to increase the cost of coverage or to add a wellness benefit, you are acting on behalf of the company. not the Plan. If, on the other hand, an employee drops an EOB on your desk and asks for your assistance clearing up a claims issue, you are assisting with Plan administration and the rules apply. As a general rule of thumb, if you receive information that relates in any way to the Plan and that includes Health Information that can reasonably be used to identify an Individual, the handling of that information must comply with the HIPAA Privacy Regulations. In all cases, if you are not sure, call the Plan's Privacy Officer for guidance.

Q4: Can I still receive summary reports of Plan information from the TPA?

A4: Probably yes, especially if the information does not identify specific individuals (De-identified information). In general, all requests for data or reports should be coordinated through the Privacy Officer or his/her designee.

IV. **Permitted Disclosures - "TPO".**

As stated above, unless otherwise permitted or required by the HIPAA policy and procedures or the Privacy Regulations, the Plan cannot Use PHI obtained from any source or Disclose PHI maintained by or in the possession or control of the Plan, unless the affected Individual has provided a prior written Authorization approving such Use or Disclosure either directly to the Plan or through a Healthcare Provider or other Covered Entity. However, the Plan can Use or Disclose PHI for its own purposes of Payment or Healthcare

Operations, as defined below, without first obtaining a Participant's Authorization. A Covered Entity, such as the Plan can also Use and Disclose PHI without a specific Authorization for Treatment purposes. Because the Plan is not a Healthcare Provider, any Use or Disclosure of PHI for Treatment purposes should occur infrequently, if at all. Together, these permissible Disclosures for Treatment, Payment and Healthcare Operations are referred to as "TPO" Disclosures, as further defined below.

"Treatment" means the provision, coordination or management of healthcare and related services by one or more Healthcare Providers, including the coordination or management of healthcare by a Healthcare Provider with a third party; consultation between Healthcare Providers relating to a patient; or the referral of a patient for healthcare from one Healthcare Provider to another.

"Payment" means the activities undertaken by the Plan to:

1. Obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Plan; or
2. Pay claims for healthcare benefits; or
3. Perform certain other Plan activities, including, but not limited to: determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication or subrogation of health benefit claims: risk adjusting amounts due based on enrollee health status and demographic characteristics; billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related healthcare data processing: review of healthcare services with respect to medical necessity, coverage under a health plan. appropriateness of care or justification of charges; utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: (1) name and address; (ii) date of birth: (iii) social security number; (iv) payment history; (v) account number; and (vi) name and address of the Healthcare Provider and/or health plan.

"Healthcare Operations" include any of the following activities of the Plan to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation (where general knowledge is not the primary purpose); population based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination: contacting Healthcare Providers and patients with information about Treatment alternatives; and related functions that do not include Treatment;

2. Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, Plan performance, training of non-healthcare professionals, accreditation, certification, licensing or credentialing activities;

3. Underwriting, premium rating and other activities relating to the creation. renewal or replacement of a contract of health insurance or health benefits, and ceding. securing or placing a contract for reinsurance of risk relating to claims for healthcare (including stop-loss insurance and excess loss insurance);

4. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Plan. Including formulary development and administration, development or improvement of methods of payment or coverage policies; and

6 Business management and general administrative activities of the Plan, including, but not limited to:

- Management activities relating to implementation of and compliance with the requirements of HIPAA:
- Customer service, including the provision of data analyses for policy holders, plan sponsors or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer:
- Resolution of internal grievances:
- The sale, transfer, merger or consolidation of all or part of the Plan with another Covered Entity, or an entity that, following such activity, will become a Covered Entity. and due diligence related to such activity: and
- Creating De-identified Health Information or a Limited Data Set. (explained in Section IX below)

Examples of TPO for which the Plan can Use or Disclose PHI include:

I. Confirming eligibility to a physician inquiring about a patient's coverage for benefits under the Plan: and

2. Troubleshooting a claims payment issue with a Healthcare Provider.

Common Questions and Answers:

Q1: Will the Privacy Rule affect how the Plan responds to questions from employees about eligibility for benefits for other covered family members?

Al: Generally, no. The Plan may continue to respond to requests from an employee for coverage information about other family members who are covered dependents under the Plan, especially if the covered dependent is a minor. (See Section VII below for additional information.) However, an Individual may request a restriction on the Plan's Use and Disclosure of that Individual's PHI, including a restriction not to release such information to other family members. If the Plan agrees to such a restriction, the Plan cannot discuss eligibility or benefits regarding that Individual with anyone else.

Q2: Can we continue to request a doctor's certification for a release to work?

A2: Yes. However, if you request that the information be supplied by the physician, the physician, as a Covered Entity, will probably require a signed Authorization to release the information. If the physician supplies the information directly to the employee and the employee gives the information to the company, no Authorization would be required.

Q3: Can the Plan use PHI in making benefit determinations upon a claims appeal?

A3: Yes, making benefit determinations is a Plan administrative function and an Individual's written Authorization is not required. However, any Use of the PHI must he restricted to the Minimum Necessary to make the claims determination. It may be possible and preferable to make claims determinations without any data identifying the individual. Regardless, the information will also have to be safeguarded once in your possession.

Q4: May I discuss PHI with a third party administrator or insurance carrier?

A4: Yes, as long as the Disclosure is necessary for Treatment, Payment or Healthcare Operations of the Health Plan.

Related Form: Authorization for Use and Disclosure of Protected Health Information V.

Other Permitted Disclosures.

The Plan can also Use or Disclose PHI without obtaining a Participant's prior written consent or Authorization in the following circumstances:

1. Emergency treatment situations.
2. As required b state or federal law: in judicial or administrative proceedings: for law enforcement purposes (for example, responding to a court or administrative order. licensure or disciplinary actions; workers' compensation or work-related injury programs).
3. Public health activities; health oversight activities (Disclosure to the FDA, CDC or other authorized agency to prevent or control disease or injury, or for public health surveillance or investigations).
4. Workers' compensation or work-related illness or injury (to state workers' compensation or federal OSHA agencies to report and coordinate work-related claims).
5. Incidental Uses and Disclosures - "Incidental" Uses and Disclosures that are made pursuant to otherwise permitted or required Uses or Disclosures are not considered Violations of the Privacy Regulations. For example, if an employee overhears a member of the Plan's Workforce discussing a Participant's claim over the phone, any Disclosure of PHI to the employee walking by is incidental and not a Violation of the Privacy Regulations. However, the Plan must make reasonable efforts to prevent and limit incidental Uses and Disclosures of PHI.

In addition, the Plan can Use PHI without specific Authorization if the PHI is either deidentified or in a Limited Data Set (see Section IX below for further information).

Common Questions and Answers:

Q1: Are there any required Disclosures of PHI?

A1: Yes, there are three required Disclosures. The Plan is required to Disclose PHI to the Individual who is the subject of the PHI, to the HHS in response to an investigation or inquiry regarding the Plan's compliance with the Privacy Regulations, and to the extent that a Use or Disclosure is required by law.

Q2: When can I Disclose PHI to the workers' compensation group?

A2: PHI may be disclosed to employees responsible for administering the company's workers' compensation program as authorized by and to the extent necessary to comply with workers' compensation laws. If you receive a request for information from the Plan to be used for workers' compensation purposes, it is important that you verify that the Disclosure is necessary under the applicable workers' compensation statute. If you have questions, check with the Plan's Privacy Officer.

VI. Disclosures Permitted With Authorization.

An Individual's Authorization for the Use or Disclosure of PHI is required whenever the Use or Disclosure is not otherwise permitted by the Privacy Regulations. An Individual may want to have his or her PHI Disclosed by the Plan for a number of reasons, including applications for life or disability insurance, or for purposes of a lawsuit or collection activities. While most requests for such information may be made to the Individual's Healthcare Provider, the Plan may occasionally receive a request to Disclose PHI.

In addition, the Plan may request a Participant's Authorization to release or Use PHI for a purpose other than TPO, or the Plan may request an Authorization that would allow another Covered Entity to Disclose information to the Plan. Finally, if the Plan wishes to Use PHI for Marketing purposes, the Plan must obtain the Participant's Authorization. In general, the Plan does not engage in any Marketing activities. (Marketing does not include advising Participants of available coverage options or providing information regarding wellness activities, health fairs or support groups or classes.)

Authorization Requirements - An Authorization to Use or Disclose PHI must be specific to the requested reason for the Authorization and generally cannot be combined with any other type of document. Authorizations must contain six basic elements:

1. A description of the information to be Used or Disclosed - the description must be specific and meaningful, such as "lab results from August 2004," "all x-ray s," or "results from Cat-scan performed in June 2004". An Individual may also Authorize the Disclosure of his or her entire medical record, if appropriate.

2.The identification of the person(s) authorized to Use or Disclose the PHI - the name or other identification of the person or class of individuals permitted to make the requested Disclosure of the Individual's PHI such as "Dr. Smith" or "Claims Supervisor at X".

3. The identification of the person(s) authorized to receive the PHI - the specific name or identification of the individual(s) authorized to receive the requested Use or Disclosure of PHI.

4. The purpose of the requested Use or Disclosure - a description of the reason for the request. If the Participant initiates the request, "at the request of the individual" is acceptable.

5. Expiration date or event - an expiration date or event related to the Participant or the reason for the Use or Disclosure of PHI, such as "December 31, 2004." "one year from the date the Authorization is signed," or "upon acceptance or rejection of my life insurance application."

6. Signature and date - the Authorization must be signed and dated by each Individual whose information will be disclosed. If a personal representative signs for an Individual, the Authorization must also include a description of the representative's authority. Electronic signatures are acceptable as long as certain standards are met.

In addition to the above requirements, the Authorization must be written in plain language and notify the Individual of the right to revoke the Authorization, the potential for redisclosure by the recipient and the fact that the Plan cannot condition Treatment, payment, enrollment or eligibility for benefits on the Individual's Authorization (unless the Authorization is requested in order to determine eligibility for coverage and certain underwriting purposes). The Plan must also provide the Individual with a copy of the signed Authorization form.

Common Questions and Answers:

Q1: When do I have to obtain an Authorization?

A1: You must obtain an Authorization if you are requested to Use or Disclose an Individual's PHI for any reason other than those Uses and Disclosures permitted by the Privacy Regulations. including the Plan's Treatment, Payment or Healthcare Operations, or release of PHI to the Individual.

Q2: Who can give an Authorization to release PHI?

A2: Individuals who can give an Authorization to release PHI are the Participant or Individual whose PHI is to be Used or Disclosed. a parent or legal guardian of a minor. a personal representative, or if the Individual is incapacitated, an Authorization can he given h\ a spouse. guardian or personal representative.

Q3: Can an Individual revoke or cancel an Authorization?

A3: Yes. The Individual may revoke or cancel an Authorization at any time and must do so in writing. However, if the Plan has acted in reliance on the Authorization or if the Authorization was obtained as a condition of obtaining coverage, any Uses or Disclosures made according to the Authorization remain permitted Uses or Disclosures of the Individual's PHI.

Related Form: Authorization for Use and Disclosure of PHI

VII. Disclosures With Opportunity To Agree Or Object.

The Plan can Use or Disclose PHI without obtaining the Individual's prior written authorization in the following circumstances: Disclosures to the Individual's family, personal representative or friends; in connection with disaster relief efforts; in emergency circumstances: or when in the best interests of the Individual when the Individual is not present or is incapable of responding. The Plan will inform the Participant in advance in its Notice of Privacy Practices of the possibility of such Uses or Disclosures, and the Participant will be given the opportunity to agree to or prevent or restrict the Use or Disclosure. As an alternative to including this in the Notice, the Plan may notify the Participant either in writing or verbally prior to each such Use and Disclosure in order to afford the Individual the opportunity to agree or object at that time.

Personal Representatives - A personal representative is a person who has the ability to act for the Individual and exercise the Individual's rights under HIPAA. The Plan must treat an authorized personal representative just like a Participant for all purposes under the Privacy Regulations and according to the powers given to the personal representative. The personal representative may have broad powers, such as a parent for a minor child or a legal guardian for a mentally incompetent adult. However, a personal representative may also have limited powers. such as a limited healthcare power of attorney with respect to artificial life support or a specific treatment. In that case, the Plan may

treat the personal representative as the Participant only with regard to that limited purpose. If a personal representative has authority to act for a deceased Individual or his or her estate, the Plan must treat the personal representative as the Participant for all purposes of the Privacy Rule. The chart below lists who must be recognized as a personal representative for each category of Individual:

If the Individual is:	The Personal Representative can be:
An Adult or An Emancipated Minor	A person with legal authority to make healthcare decisions on behalf of the Individual Examples: Healthcare power of attorney Court-appointed legal guardian General power of attorney
An Unemancipated Minor	A parent, guardian or other person acting *in loco parentis* with legal authority to make healthcare decisions on behalf of the minor child - see section below regarding Parents and Minors
Deceased	A person with legal authority to act on behalf of the decedent or the estate (not restricted to healthcare decisions) Examples: Executor of the estate Next of kin or other family member Durable power of attorney

Parents and Minors - In general, the Privacy Regulations defer to state law to determine when a parent, guardian or other person may obtain Health Information on a minor child. In most cases, the parent is the personal representative and can exercise the child's HIPAA Privacy rights. However, there are three circumstances when the parent is not the personal representative for the child:

1. When state or other law does not require parental consent before a minor can obtain certain healthcare services and the minor consents to the care.

   Example: A state law permits an adolescent to obtain mental health treatment without parental consent and the adolescent consents to such treatment without the parent's consent.

2. When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor.

   Example: A court grants authority to make healthcare decisions for a minor to another adult, or the court makes the decision itself.

3. When a parent agrees to a confidential relationship between the minor and a healthcare provider.

Example: A doctor asks the parent of a 16-year old if he can talk to the child confidentially about a medical condition and the parent consents.

Common Questions and Answers:

Q1: When can I Disclose PHI to a personal representative?

A1: A personal representative is to be treated the same as an Individual, so you may disclose an Individual's PHI to his or her personal representative upon proper request. You should verify the person's authority to act on behalf of the Individual as a personal representative before you disclose any PHI.

Q2: When can I Disclose PHI about deceased individuals?

A2: Information about deceased individuals may be disclosed to an appropriate personal representative upon proper request.

Q3: If someone has a healthcare power of attorney for an Individual, can they obtain Access to the person's PHI?

A3: Yes. If a person has a healthcare power of attorney, the representative has the right to Access PHI of the Individual they are representing to the extent permitted by the Privacy Regulations.

Q4: Who is a "family member or close personal friend"?

A4: The Privacy Regulations' list of family members and close personal friends is generally broad and includes, but is not limited to, blood relatives, spouses, roommates, boyfriends, girlfriends, domestic partners and neighbors. However, the "close personal friend" exception should be read narrowly so that any disclosure is made only to those individuals with the closest relationship to the Individual. Also, any disclosures must still meet the Minimum Necessary standards required by the Privacy Regulations. Employers or employer representatives are not generally "close personal friends".

VIII. Disclosure Procedures And Restrictions.

Minimum Necessary -The Plan will comply with the Minimum Necessary standard with respect to any Use or Disclosure of, or request for, PHI, as required by the Privacy Regulations. This means that all Uses or Disclosures of, or requests for, PHI will be limited to the minimum amount necessary to accomplish the stated purpose or will be in conformity with such other restrictions as the Plan may have agreed to with certain Participants. The Plan has developed criteria designed to limit its requests for PHI to the information reasonably necessary to accomplish the purposes for which the request was made. An entire medical record may not he Used, Disclosed or requested except where specifically justified as the amount that is reasonably necessary to accomplish the stated purpose. However, the Plan can Use and Disclose PHI for Payment, Healthcare Operations, pursuant to an Authorization or as required by law without complying with this requirement. The Plan will make reasonable efforts to limit

access to PHI by its Workforce and otherwise within its operations only to authorized personnel.

The Minimum Necessary standard does not apply to the following:

1. Disclosures to a Healthcare Provider for Treatment purposes:

2. Disclosures to an Individual who is the subject of the PHI:

3. Uses or Disclosures made pursuant to an Individual's Authorization:

4. Uses or Disclosures required for compliance with HIPAA:

5. Disclosures to HHS when Disclosure is required for enforcement purposes: and

6. Uses or Disclosures required by other law.

Business Associate Agreements - The Plan has or will execute Business Associate agreements with any persons or entities performing functions on behalf of the Plan to the extent they create or receive PHI from or on behalf of the Plan in connection with performing those functions. Some of the Plan's Business Associates may be third party administrators, consultants, actuaries, brokers and outside law firms that handle claim disputes. The existence of a Business Associate agreement does NOT permit the Plan to freely Disclose PHI to a Business Associate where an Authorization would otherwise be required and does not relieve the Plan from its obligations under the Privacy Regulations to only Use or Disclose PHI as permitted or required by the Privacy Regulations. The Privacy Officer is responsible for determining who is a Business Associate and for entering into agreements with those Business Associates.

Mitigating Harm - The Plan must mitigate to the extent possible, any harmful effect that the Plan knows resulted from an improper Use or Disclosure of an Individual's PHI.

Common Questions and Answers:

Q1: When can I Disclose PHI to a Business Associate?

Al: You may Disclose PHI to a Business Associate of the Plan upon the receipt of a proper request. The Disclosure must be limited to the Minimum Necessary standard and must be one of the types of Disclosures permitted in the Business Associate Contract with the individual Business Associate.

Q2: Who are the Plan's Business Associates?

A2: Business Associates are typically outside vendors that perform services for the Plan. For a complete list of the Plan's Business Associates, contact the Privacy Officer.

Q3: What do I do if I think the Plan has improperly Used or Disclosed PHI?

A3: If you know or believe that a Violation of the Plan's HIPAA privacy policy and procedures has occurred, contact the Plan's Complaint Officer or the Privacy Officer.

Q4: How do I decide what is the "Minimum Necessary" amount of information to Disclose?

A4: You must use reasonable efforts to limit Disclosures to the minimum amount of information

necessary to complete the stated purpose or reason for the Disclosure. However, if the Disclosure is in response to a request from a Business Associate or another Covered Entity, you may reasonably rely on the request as meeting the Minimum Necessary standard.

IX. **De-identified Information.**

De-Identified PHI - Under the Privacy Regulations, De-identified Health Information is not individually identifiable and, therefore, is not PHI. The Plan can use and disclose deidentified Health Information without complying with the requirements of the regulations, including the requirement to obtain a Participant's prior written Authorization. There are two permitted methods of De-identification under the Privacy Regulations: "statistical deidentification" or the removal of the 18 identifiers enumerated in the Privacy Regulations. The Plan may assign a code to the De-identified Health Information to permit it to Re-identify the data. However, the key to the Re-identification code may not be disclosed and the recipient can not be able, through the use of known information about the individual, for example to determine the identity of the individual or the key to Re-identify the data.

Limited Data Set De-Identification - The Plan can use or disclose PHI in a Limited Data Set, without completely De-identifying the information or obtaining a Participant's prior written Authorization, but only for purposes of public health or certain Healthcare Operations. If the Plan engages in either of these two activities, the Plan will remove all of the following direct identifiers of the Individual and/or the Individual's family, employers or household members prior to Disclosing the information (unless the Disclosure is made to an agent or Business Associate who will remove the identifiers on the Plan's behalf): name, postal address information (other than town or city, State and zip code), telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, Web Universal Resource Locators (URLs), Internet Protocol JP) address numbers, biometric identifiers including finger and voice prints, and full face photographic images or any comparable images.

Before disclosing any information containing Limited Data Sets, the Plan will first enter into a Data Use Agreement with the recipient of the information. The Plan's Data Use Agreements will comply with the requirements of the Privacy Regulations and will contain assurances of protection of the information, an agreement not to re-disclose, an agreement not to identify or contact the Individual who is the subject of the Disclosed information, and what the permitted Uses and Disclosures are, as well as a list of any permitted recipients. The recipient *will* also agree to notify the Plan of any improper Uses or Disclosures.

Common Questions and Answers:

Q1: When can I use De-identified or summary Health Information?

A1: If the information has been De-identified, it may generally be disclosed fully. Example: a potential new carrier requests past claims data in De-identified form to underwrite the risk. If the information is a Limited Data Set, you must ensure that a Data Use Agreement is in place before you release any information. The Privacy Officer is solely responsible for ensuring that the requirements are met.

X. Participant Rights.

Under HIPAA, Participants have certain rights regarding their PHI. These rights include (1) a right to Access one's own PHI contained in a Designated Record Set, (2) the ability to amend one's own PHI. (3) the right to request an accounting of the Uses and Disclosures of ones own PHI, (4) the right to request restrictions on the use of PHI and (5) the right to request Confidential Communications.

1. ***Designated Record Sets/Access*** **-** The Plan maintains for each Individual a "Designated Record Set" that is subject to Access by the Individual to whom the information pertains. The Designated Record Set is the set of records maintained by the Plan that includes the Individual's PHI. An Individual must make a written request to the Plan to Access his or her PHI. The Plan must respond to the Access request within 30 days if the PHI is maintained on site, or within 60 days if the PHI is maintained off site. In most cases, the PHI \ill he maintained by the Plan's Business Associates off site, so it is reasonable to expect that the Plan will respond to an Individual's request for Access to PHI within 60 days. If the Plan cannot provide the Access requested within 60 days, the deadline can be extended for an additional 30 days if the Plan tells the Individual within the initial 60-day period that an extension is needed and the date by which the Plan will provide the requested Access.

• ***Format of Information.*** If the Plan grants the Individual's request for Access to his or her PHI, the Plan must provide the information in the format requested by the Individual. or if the information is not available in the format requested, in a readable hard copy of another format agreed to between the Plan and the requesting Individual. If the Individual agrees, the information can be reported in a summary. The Plan can charge a reasonable fee for copying, mailing or summarizing the requested information.

• ***Denials of Access Permitted.*** An Individual's right of Access to his or her Designated Record Set can be denied by the Plan. without the right to contest the denial, with respect to Psychotherapy Notes, information compiled for civil, criminal or administrative actions, information subject to the Federal Privacy Act 5 USC §552(a), and information obtained by the Plan from another entity under a promise of confidentiality if Access would be likely to reveal the source of the information.

An Individual's Access to his or her Designated Record Set can also be denied by the Plan, provided the Individual has a right to contest the denial, when the Plan determines, in its discretion, that Access by the Individual or the Individual's representative is reasonably likely to endanger the life or physical safety of the Individual or another person identified in the PHI.

• ***Notice of Access Denial.*** If the Plan denies an Individual's request to Access his or her PHI, the Plan must provide the Individual with a written notice telling the Individual the basis for the denial, whether the Individual has a right to contest the denial and a description of the Plan's complaint procedure regarding HIPAA Privacy Violations.

2. ***Amendment of Protected Health Information*** **-** An Individual has the right to have the Plan amend his or her PHI (or a record about the Individual contained in the Plan'; Designated Record Set) for as Ion- as the information is maintained in the Designated Record Set. The Plan requires that requests for amendment be made in writing and provide a reason to support the requested amendment. The Plan must act on such a request within 60 days after receipt of the request. This time limit may be increased once by no more than 30

days if the Plan provides the Individual with a written statement of the reasons for the delay and the date with which the Plan will complete the action requested.

• ***Amending the Record.*** If the Plan grants the Individual's request to amend, the Plan must: (1) make the amendment, at a minimum appending the requested amendment to the proper location in the records, (2) inform the Individual that the amendment was accepted, (3) obtain the Individual's identification of and agreement to have the Plan notify relevant persons with whom the amendment needs to be shared and (4) make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the Individual as having received the PHI prior to the amendment, as well as persons that the Plan knows hake the PHI that has been amended and that may have relied, or could foreseeably rely, on it to the detriment of the Individual.

• ***Denial of Request to Amend.*** The Plan can deny an Individual's request to amend his or her records if the information was not created by the Plan, it is not part of the Participant's Designated Record Set, would not otherwise be Accessible to the Individual, or the information is accurate and complete. If the Plan denies the Individual's request to make the amendment, it must:

(a) Provide the Individual with a written denial within 60 days, as specified above, stating (i) the basis for the denial, (ii) the Individual's right to submit a written statement disagreeing with the denial and how to file this statement, (iii) that if the Individual does not submit a statement of disagreement, the Individual may request that the Plan attach the Individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment and (iv) how the Individual may complain to the Plan pursuant to the Plan's complaint procedures, including the name or title and telephone number of the Plan's HIPAA contact person or office, or how to complain to the Secretary of HHS.

(b) Provide the Individual with the ability to submit a written statement of disagreement with the denial and the basis of such disagreement. The Plan may prepare a written rebuttal to the Individual's statement of disagreement and provide a copy to the Individual.

(c) Identify the record or PHI in the Designated Record Set and append or otherwise link the Individual's request for an amendment, the Plan's denial, the Individual's statement of disagreement and the Plan's rebuttal, to the Designated Record Set.

If a statement of disagreement has been submitted by the Individual, the Plan must include items appended to the record with any subsequent Disclosure. However, if the Individual has not submitted a written statement of disagreement, only at the request of the Individual is the Plan required to include the Individual's request for amendment and the Plan's denial, or an accurate summary thereof, with any subsequent Disclosure of the PHI. If the Plan is informed by another Covered Entity that an amendment to PHI has been made, the Plan must make or append the amendment to the records in its possession or control.

3. ***Accounting of Disclosures*** - The Plan must provide an accounting to an Individual of certain Disclosures of PHI made during periods up to 6 years prior to the date of the Individual's request. Requests for an accounting must be made to the Plan in writing. The Plan must respond to a request for an accounting within 60 days. This period may be extended for another *30* days if the Plan tells the Individual of the delay, including the reason and the date that the information will be provided. The first accounting in any 12-month period must he provided to the Individual free of charge. The Plan can charge reasonable cost-based fees for any subsequent accountings in the same 12-month period. The Plan must document the information required to be included in an accounting, the written accounting provided to the Individual and titles of persons or officers responsible for receiving and processing requests for an accounting.

An accounting also must include Disclosures of PHI made by the Plan's Business Associates, and for each Disclosure the Plan must report the date of the Disclosure, name of the entity or person who received the PHI and, if known, the person's address, a brief description of the PHI Disclosed and a brief statement of the purpose of the Disclosure. If multiple Disclosures are made to the same entity or person for a single purpose then the accounting may include: the information provided above for the first disclosure during the accounting period, the frequency, or number of the Disclosures made during the accounting period, and the date of the last such Disclosure during the accounting period.

The Plan is not required to account for Disclosures made to the Individual regarding his or her own PHI; for purposes of Treatment, Payment or Healthcare Operations: incident to an otherwise permitted Use or Disclosure; pursuant to an Authorization: as otherwise required h\ law or the Privacy Regulations as part of a Limited Data Set; or with respect to Uses or Disclosures that occurred prior to April 14, 2004.

4. ***Restriction of Uses and Disclosures*** **-** An Individual has the right to request the Plan to restrict the Use and Disclosure of the Individual's PHI. The Plan requires that such a request be made in writing to the Plan. The Plan is not required to agree to any requested restrictions. However, if the Plan agrees to a specific restriction, the[y] Plan cannot use the Individual's PHI in violation of the agreed-upon restriction. For instance, an Individual may request that the Plan not disclose PHI to any family members.

5. ***Confidential Communications*** **-** An Individual has the right to request Confidential Communications from the Plan. The Plan requires that such requests be made in writing and the Plan must accommodate reasonable requests for such communications. A Confidential Communication is a communication of PHI made by the Plan in an alternative means or to an alternative address or location. For instance, a covered spouse may request that Plan information or EOBs be sent to a work address and not to the Individual's home. The Plan cannot require the Individual to explain the reason for the request for Confidential Communications as a condition of granting the request.

Common Questions and Answers:

Q1: All of the records are at the third party administrator; what records do disclose if a Participant requests Access?

A1: Only what is available. Assuming there are no records, you should refer the Participant to the appropriate Business Associate to request the information.

Q2: Who can request a restriction on the Use and Disclosure of PHI?

A2: Any Individual may request a restriction on the Use or Disclosure of his or her own PHI by submitting a written request to the Plan describing the requested restriction, however. the Plan does not have to agree to the requested restriction. If the Plan does agree to the restriction, the restriction must be properly documented and all future Uses and Disclosures must be made according to the restriction.

Q3: What kinds of restrictions can an Individual place on the Use or Disclosure of PHI?

A3: An Individual may request that certain PHI not be Used or Disclosed for certain purposes or to certain other individuals or entities. For example, an Individual may request that no Disclosures be made to a spouse.

An Individual may not request any restrictions on the Use or Disclosure of PHI if the Use or Disclosure is one that is permitted by the Privacy Regulations without an Authorization or the Individual's ability to agree or object. In addition, an individual may not request a restriction on Disclosure to the HHS.

Q4: When can I deny an Individual's request for Access to his or her PHI?

A4: You can generally deny an Individual's request for Access to PHI in three circumstances: (i) if the request is for Psychotherapy Notes, (ii) if the PHI was obtained from an entity other than a Healthcare Provider under a promise of confidentiality or (iii) if a licensed Healthcare Provider determines that release of the PHI to the Individual is reasonably likely to endanger the life or physical safety of the Individual or another person.

Q5: What information can an Individual request to amend in his or her PHI?

A5: The Individual may amend any of his or her PHI contained in the Designated Record Set. The Individual must make a written request to the Plan describing the amendment and provide a reason to support the requested amendment.

Q6: What Uses and Disclosures do I have to include in an accounting?

A6: An accounting must include Uses and Disclosures of PHI that do not fall into one of the following categories: (i) a Use or Disclosure for Treatment, Payment or Healthcare Operations; (ii) a Disclosure to the Individual of his or her own PHI; (iii) incidental Disclosures. if the Disclosure is otherwise permitted by the Privacy Regulations; (iv) Uses and Disclosures made according to an Authorization; (v) Uses or Disclosures made as part of a Limited Data Set: and (vi) Uses and Disclosures made prior to April 14. 2004. In short, it is likely that there will be no Uses or Disclosures that the Plan must account for to an Individual as they should generally be for Payment or Healthcare Operations.

Related Forms: -Access to Designated Records Request

-Amendment of Designated Records Request
-Accounting of Disclosures of PHI

XI. Safeguarding, Handling, Storage And Retention.

In addition to administrative policies and procedures safeguarding the Uses and Disclosures of PHI, HIPAA requires the Plan to create technical and physical safeguards. These safeguards are especially important when employees wear "multiple hats" and must he careful not to disclose PHI outside of their Plan administrative duties.

Technical safeguards may include limiting access to PHI by creating computer fire% ails. restricting e-mail proxy rights, encrypting e-mail or other similar means of protecting PHI, including setting up designated e-mail and voicemail boxes to receive inquiries and complaints, with access restricted to authorized persons.

Physical safeguards may include separate files and locking filing cabinets for PHI and Plan data, locking office doors, a dedicated computer, methods of destruction of PHI and similar document control procedures.

PHI must be stored in secure locations and maintained for a minimum of six years. Also, the Plan

must have procedures for the appropriate destruction of PHI when appropriate.

Common Questions and Answers:

Q1: Does this mean that I have to clean my work area before I go home?

Al: Generally, yes. Data and information that contains PHI should be secured at the end of the day. If it is not possible to close and lock an office door to restrict access to the area, this may mean putting papers in a locking file cabinet or desk. Cleaning people or others walking by the area cannot have improper access to PHI.

XII. Complaint Procedure.

The Plan has created a process for Individuals to make complaints regarding the Plan's HIPAA privacy policy and procedures and for perceived Violations of those practices. The Plan requires that complaints be made in writing. All complaints should be forwarded to the Plan's Complaint Officer for review, investigation and response. The Plan can not retaliate, intimidate. threat or discriminate against any Individual making a complaint or otherwise exercising his or her HIPAA Privacy rights.

Common Questions and Answers:

Q1: Who is the Complaint Officer?

A l : The Director of Human Resources is the designated Complaint Officer.

Q2: If an Employee comes to me with a complaint, what do I do?

A2: Refer the employee to the Complaint Officer to decide if the complaint should be documented. If determined necessary, there is a form that will be completed.

Related Form: Complaint Form

XIII. Notice Of Privacy Practices.

The Plan has developed a Notice of Privacy Practices (the "Notice") that describes the Plan's policy and procedures for handling PHI. The Notice advises Participants of when and why the Plan may Use or Disclose PHI, the Individual's lights and the Plan's legal duties with regard to PHI. The Plan must provide the Notice to all individuals enrolled in the Plan - a single notice to the Participant (covered employee) is effective for all covered dependents.

The initial Notice must be provided to all Participants no later than April 14, 2004. After the initial compliance date, the Notice must be given to all new employees when they enroll in the Plan and within 60 days of a material change in the Notice. Every three years the Plan must remind Participants that the Notice is available and tell Participants how they may request or obtain a copy of the Notice.

Common Questions and Answers:

Q1: When do I have to give the Notice of Privacy Practices?

Al: The initial Notice will be distributed to all Plan Participants no later than April 1 2004. After the initial notice period, the Notice must be given to individuals at the time that the% enroll in the Plan. New hire materials will be amended by April 14, 2004 to include the Notice as a standard item. Once every three years, the Plan also must notify Participants that the Notice is available for review and tell Participants how they can obtain a copy of the Notice.

Q2: What if the Plan's HIPAA Privacy Practices change?

A2: If there is a material change to the Plan's HIPAA Privacy Practices, a revised Notice must be given to all Plan Participants within 60 days of the change. The Privacy Officer will ensure this occurs.

Q3: How do I have to deliver the Notice?

A3: The Notice may be delivered by hand or by mail. The Notice may also be delivered by e-mail if the individual agrees to an electronic Notice, if the Plan maintains a website. the Notice must be prominently posted on the website, as well.

Q4: Do we have to have a signed receipt of Acknowledgement that the individual received the Notice?

A4: No, health plans are not required to obtain a signed Acknowledgement that the individual received the Notice. However, if the Notice is distributed at the time of new hire orientation or Plan enrollment, it will be easy to request an Acknowledgement. A form has keen prepared for this purpose.

Related Forms:

- Notice of Privacy Practices
- Acknowledgement of Receipt of Notice of Privacy Practices

XIV. **Responsible Parties.**

The Plan has designated a Privacy Officer and a Complaint Officer. The Privacy Officer is responsible for developing and implementing policies and procedures to assure that the Plan complies with the HIPAA Privacy Regulations. The Complaint Officer is responsible for receiving, investigating and responding to complaints about Violations of the Plan's HIP.-AA Privacy Practices. Other individuals may be designated as contact persons to receive a Participant's requests for Access to, amendments to, or accountings of PHI.

Common Questions and Answers:

Q1: Who is the Plan's Privacy Officer?

Al: The Director of Human Resources or if that position is vacant, or the individual is unavailable, contact the Business Office.

Q2: Who is the Plan's Complaint Officer?

A2: The Director of Human Resources.

Q3: Where can I get more information about the Plan's HIPAA privacy policy and procedures?

A3: A complete copy of the Plan's HIPAA privacy policy and procedures are available at the Department of Human Resources; you may also contact the Plan's Privacy Officer or Complaint Officer for additional information.

Q4: Do I need to post the Privacy Notice on the Web

A4: **Yes,** the Notice of Privacy Practices should be posted on your intranet site, applicable.

Q5: Do we need to update the Notice?

A5: Yes, the Notice must be updated every 3 years or sooner if the Plan's practices and procedures change. The Privacy Officer is responsible for all updates to the Notice.

XV. Glossary .

The following are definitions of key terms used in this manual and the corresponding HIPAA privacy policy and administrative and implementing procedures. *Any* terms used in this manual or the policy or corresponding administrative and implementing procedures, but not otherwise listed or defined below, have the meanings given them in the standards for Privacy of Individually Identifiable Health Information: Final Rule, Federal Register, Vol. 67, No. 157. August 14, 2002, 45 CFR Parts 160 and 164.

1.1 **Access** means an Individual's right to inspect and obtain a copy of his or her own PHI contained in a Designated Record Set maintained by the Plan.

I.2 **Acknowledgement** means the written documentation of an Individual's receipt of the Plan's Notice of Privacy Practices.

1.3 **Authorization** means the written permission from an Individual that permits the Plan to Use or Disclose PHI for purposes other than Treatment, Payment or Healthcare Operations.

1.4 **Business Associate** means a person or entity who is not a member of the Plans Workforce and who, on behalf of the Plan:

(a) Performs or assists in the performance of a function or activity involving the Use or Disclosure of PHI, including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing, or any other function or activity regulated by HIPAA: or

(b) Provides legal, actuarial, accounting, consulting, data aggregation (as defined in HIPAA), management, administrative, accreditation, or financial services to or for the Plan, where the provision of the service involves the disclosure of Individually Identifiable Health Information from the Plan, or from another Business Associate of the Plan, to the person.

I.5 **Business Associate Contract** means the contract between the Plan and its Business Associate that allows the Business Associate to create or receive PHI on behalf of the Plan.

I.6 **Complainant** means an Individual who reports a privacy-related complaint to the Plan.

1.7 **Complaint Officer** means the person or official designated by the Plan to receive and process privacy-related complaints.

1.8 **Confidential Communication** means a communication regarding PHI between an Individual and the Plan that is sent through alternative means or to an alternative location from the regular method of communication.

1.9 **Covered Entity** means:

(a) A Health Plan.

(b) A healthcare clearinghouse.

(c) A Healthcare Provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA privacy rules.

1.10 **Data Use Agreement** means a required agreement between the Plan and a Limited Data Set recipient setting forth the requirements and limitations for the Use or Disclosure of the PHI in the LDS that the recipient must follow, and the consequences for not following them.

1.11 **De-identification Determination** means a written assessment provided by a statistical expert that attests that he/she has determined that the risk is very small that the information in a specific data set could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information.

1.12 **De-identify** or **De-identification** means that a data set containing PHI has been determined to be De-identified by a statistical expert or that it has been modified by removing 18 specific PHI identifiers. In either case, there is no reasonable basis to believe that the information in the data set can he used to identify an Individual.

1 13 **Designated Record Set** means a group of records maintained by or for the Plan that is: (i) the medical records and billing records about Individuals maintained by or for a covered Healthcare Provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan; or (iii) used, in whole or in part, by or for the Plan to make decisions about Individuals.

1.14 **Disclose** or **Disclosure** means, with respect to PHI, the release, transfer, provision of Access to, or divulging in any other manner, PHI outside of the Plan's internal operations or its Workforce Members.

1.15 **Group Health Plan** (also see definition of *Health Plan)* means an employee welfare benefit plan, including insured and self-insured plans, provided by an employer (or a union) for employees (and retirees, if applicable) and their dependents, that provides medical care (including dental, vision, mental health, etc.), including items and services paid for as medical care, to employees (and retirees. if applicable) or their dependents, directly or through insurance, reimbursement, or otherwise, and that (1) has 50 or more participants; or (2) is administered by an entity other than the employer that established and maintains the plan.

1.16 **HHS** means the Department of Health and Human Services.

1.17 **Healthcare Provider** means a provider of medical or health services, and any other person or organization that furnishes, bills, or is paid for healthcare in the normal course of business.

1.18 **Health Information** means any information, whether verbal or recorded in any form or medium, that (1) is created or received by a Healthcare Provider, Health Plan. Public Health Authority, employer, life insurer, school or university, or healthcare clearinghouse. and (2) relates to the past, present or future physical or mental health or condition of an individual. the provision of healthcare to an individual: or the past, present or future payment for the provision of healthcare to an individual.

1.19 **Health Insurance Issuer** means an insurance company, insurance service or insurance organization (including an HMO) that issues health insurance coverage and that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a Group Health Plan.

1.20 **Healthcare Operations** means any of the following activities of the Covered Entity to the extent that the activities are related to covered functions:

(a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of Healthcare Providers and patients with information about treatment alternatives; and related functions that do not include treatment:

(b) Reviewing the competence or qualifications of healthcare professionals. evaluating practitioner and provider performance, Health Plan performance. conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as Healthcare Providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities;

(c) Underwriting, premium rating, and other activities relating to the creation. renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for healthcare (including stop-loss insurance and excess of loss insurance);

(d) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs:

(e) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies: and

(f)Business management and general administrative activities of the entity. including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of HIPAA:
(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that Protected Health Information is not disclosed to such policy holder, plan sponsor, or customer:
(iii) Resolution of internal grievances:
(iv) The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity: and
(v) Consistent with the applicable requirements of HIPAA, creating deidentified health Information or a Limited Data Set. and fund raising for the benefit of the Covered Entity.

1.21 **Health Oversight Agency** means an agency or authority of the United States, a state. a territory, a political subdivision of a State or territory. or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency% including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the healthcare system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance. or to enforce civil rights laws for which health information is relevant.

1.22 **Health Plan** means an individual or group plan that provides, or pays the cost of. medical care.

(a) **Health plan** includes, but is not limited to, the following: a Group Health Plan.
as defined above, a Health Insurance Issuer, as defined above, and an HMO.

(b) **Health plan** excludes any policy, plan or program to the extent that it provides, or pays for the cost of, accident, disability income, supplemental liability, automobile, medical payments or other benefits for medical care that are secondary or incidental to other insurance benefits: and a government-funded program (other than one listed in HIPAA), whose principal purpose is other than providing, or paying the cost of healthcare, or whose principal activity is the direct provision of healthcare to persons or the making of grants to fund the direct provision of healthcare to persons. In addition, any health related program that is not sponsored or paid for by the employer and that is only made available for voluntary _use (on an after-tax basis) is not covered.

1.23 **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, and the regulations issued thereunder, including, but not limited to, 45 C.F.R. Parts 160 and 164.

1.24 **Individual** means the person who is the subject of Protected Health Information and who is also a Participant or former Participant in the Plan or a covered spouse, dependent or beneficiary under the Plan.

1.25 **Individually Identifiable Health Information** is information that is a subset of health information, including demographic information collected from an individual. and:

(a) Is created or received by a Healthcare Provider, Health Plan, employer, or Healthcare Clearinghouse: and

(b) Relates to the past, present, or future physical or mental health or condition of an Individual: the provision of healthcare to an Individual: or the past, present, or future payment for the provision of healthcare to an Individual: and

(i) That identifies the Individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

1.26 **Law Enforcement Official** means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law,

1.27 **Limited Data Set** or ("LDS") means a data set for Use and Disclosure of PHI for the purposes of public health or Healthcare Operations that is not completely deidentified. The data set excludes 16 specified identifiers in accordance with applicable law but includes complete dates, city or town, and five digit zip codes.

1.28 **Marketing** means a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service. Marketing does not include communications made by the Plan to describe a health related product or service or payment for a product or service that is provided or included in

the Plan's benefits; for treatment; or for case management or care coordination. If there is an arrangement between a Covered Entity and such other entity whereby the Covered Entity Discloses PHI to the other entity, in exchange for direct or indirect remuneration by an entity or its affiliate, Marketing also means to make a communication about an entity's own product or service that encourages recipients of the communication to purchase or use that product or service.

1.29 **Minimum Necessary** means the least amount of PHI needed to accomplish the intended purpose of a Use, Disclosure or request.

1.30 **Notice of Privacy Practices** or **Notice** means the Notice of Privacy Practices which describes the Plan's Uses and Disclosures of PHI.

1.31 **Opportunity to Agree or Object** means Individuals will have the opportunity in advance to agree or object to their PHI being Used or Disclosed to third parties involved in their care or Payment for such Individuals' care, for notification purposes and for disaster relief purposes. The Individual may prohibit or restrict the Disclosure.

1.32 **Participant** means the employee or former employee who is eligible to be and is covered under the Plan by reason of his or her employment relationship.

1.33 **Payment** means:

(a) The activities undertaken by:

(l)A Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Health Plan; or
(ii)A Healthcare Provider or Health Plan to obtain or provide reimbursement for the provision of healthcare; and

(b) The activities in paragraph (a) of this definition relate to the Individual to whom healthcare is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
(ii)Risk adjusting amounts due based on enrollee health status and demographic characteristics;
(iii) Billing, claims management, collection activities, obtaining Payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing;
(iv) Review of healthcare services with respect to medical necessity, coverage under a Health Plan, appropriateness of care, or justification of charges;
(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
(vi) Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:

(A) Name and address,

(B) Date of birth,

(C) Social security number,

(D) Payment history,

(E) Account number, and
(F) Name and address of the Healthcare Provider and/or Health Plan.

1.34 **Plan** means the components of the Health Plan of the Upper Ohio Valley-Mountain State Blue Cross/Blue Shield that are subject to HIPAA (See Appendix A). Whenever reference is made to the Plan's action, the activities of the Plan Sponsor on the behalf of the Plan shall be treated as the action of the Plan.

1.35 **Plan Sponsor** means Bethany College and employees and agents of the company who are responsible for Plan administration functions.

1.36 **Privacy Officer** means the person(s) or officer(s) designated by the Plan to oversee compliance with policies and procedures and with HIPAA generally.

1.37 **Protected Health Information ("PHI")** means Individually Identifiable Health Information transmitted by electronic media or is transmitted or maintained in any other form or media..

1.38 **Psychotherapy Notes** means notes recorded (in any medium) by a Healthcare Provider who is a mental health professional, documenting or analyzing the contents of conversations with individuals during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the Individual's medical record. The definition of Psychotherapy Notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of Treatment furnished, results of clinical tests and any summary of the following items: diagnosis, functional status, Treatment plan, symptoms, prognosis and progress to date.

1.39 **Public Health Authority** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

1.40 **Re-identify** or **Re-identification** means that a De-identified data set is modified so that the identities of the Individuals represented in the data set is restored.

1.41 **Treatment** means the provision, coordination or management of healthcare and related services by one or more Healthcare Providers, including the coordination or management of healthcare by a Healthcare Provider with a third party: consultation between Healthcare Providers relating to a patient: or the referral of a patient for healthcare from one Healthcare Provider to another.

1.42 **Use** or **Uses** means, with respect to PHI, the sharing, employment, application, utilization, examination or analysis of such information within the Plan's internal operations or to a member of the Plan's Workforce.

1.43 **Violation** means a violation of the Plan's privacy-related policies or any of the provisions of HIPAA.

1.44 **Workforce** or **Workforce Member** means employees and other persons whose conduct, in the performance of work for the Plan, is under the direct control of the Plan or Plan Sponsor on behalf of the Plan, whether or not they are paid by the Plan or Plan Sponsor.

APPENDIX A

The benefit programs listed on Appendix A are those portions of the *Health Plan of the Upper Ohio Valley-Mountain State Blue Cross/Blue Shield* (the "Plan") subject to the HIPAA Privacy Regulations. Other programs contained in the Plan, such as life insurance and disability coverage, if any, are not covered by HIPAA.

MEDICAL PROGRAMS

-
-
-
-
-

PRESCRIPTION DRUG PROGRAMS

-
-

Health Plan of the Upper Ohio Valley-Mountain State Blue Cross/Blue Shield
(the "Plan")

CERTIFICATION AND AGREEMENT OF COMPLIANCE WITH PRIVACY POLICIES AND PROCEDURES

I certify that:

1. I have received and reviewed a copy of the Training Manual that outlines the Plan's privacy policies, including policies related to[y] the Health Insurance Portability and Accountability Act ("HIPAA") privacy regulations.

2. I understand that after reviewing the Training Manual, I have had the opportunity to ask questions regarding the Plan's policies and procedures and that all of my questions have been answered to my satisfaction. In the event any future questions or concerns about privacy or HIPAA should arise, I agree to contact the Privacy Officer to discuss such issues.

3. I agree specifically to act in accordance with the Plan's HIPAA policies and procedures as described in the Training Manual made available to me. I understand that I may be subject to disciplinary action, up to and including termination, for violating these policies or failing to report any violation of these policies.

Signature: _____

Print Name: _____

Position: _____

Date: _____