*Effective **4/14/2004***

PRIVACY POLICY FOR THE HOPE COLLEGE EMPLOYEE BENEFIT PLAN

I. INTRODUCTION

Hope College (the "College") sponsors the Hope College Employee Benefit Plan (the "Plan") to provide certain benefits to eligible employees (the "covered employee"). The Plan provides group health care among other benefits to covered employees, their spouses, and dependents (an "individual"). For purposes of this Privacy Policy, the term "Plan" will mean only those provisions providing group health plan benefits, which include medical spending accounts, hospitalization, basic medical coverage, prescription drug, dental coverage, and vision coverage.

The College intends to comply fully with the Privacy Rule requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Since members of the College's workforce may have access to the individually identifiable health information of an individual for administrative functions of the Plan on behalf of the either the Plan or the College, all members of the College's workforce who have access to protected health information must comply with this Privacy Policy.

Protected Health Information. Protected health information ("PHI") means information that:

- is created or received by the Plan and relates to the
    - past, present, or future, physical or mental health or condition of an individual;
    - provision of health care to an individual; or
    - past, present, or future payment for the provision of health care to an individual; and
- identifies or can reasonably be used to identify an individual.

PHI includes information of persons living or deceased. PHI does not include information the College gathers in its role as an employer, including the administration of disability and life insurance, and employer policies and practices such as workers' compensation, or FMLA.

Insurers. Some of the health benefits provided by the Plan are administered by insurers. This Privacy Policy does not apply to PHI in the control of the insurance companies, nor do the privacy policies of the insurance companies apply to the College.

II. PLAN'S RESPONSIBILITIES AS COVERED ENTITY

A. Privacy Officer and Contact Person

The Director of Human Resources will be the Privacy Officer for the Plan. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy. The Benefits and Compensation Manager will serve as the contact person for covered employees who have questions, concerns or complaints about the privacy of their PHI.

B. Workforce Training

The Privacy Officer will develop training schedules and programs so that all employees who have access to PHI receive the training necessary and appropriate to permit them to carry out their functions within the Plan.

C. Technical and Physical Safeguards and Firewall

The College will establish appropriate technical and physical safeguards on behalf of the Plan to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. These safeguards include:

- Locking filing cabinets and limiting the number of employees with keys to such cabinets;
- At the end of the business day, locking door to room in which filing cabinets are located;
- Limiting the number of employees who will have access to PHI;
- Private offices or work stations for employees with access to PHI; and
- Locked, fireproof cabinets to store PHI separately from employee personnel files.

The College will establish firewalls to ensure that only authorized employees will have access to PHI and that these authorized employees:

- will have access to only the minimum amount of PHI necessary for plan administrative functions, and
- will not further use or disclose PHI in violation of HIPAA's privacy rules.

D. Privacy Notice

1. Benefits Administered by Us

The Privacy Officer is responsible for developing and maintaining a notice of privacy practices (the "Notice") for the Plan and distributing the Notice to all concerned workforce members. The Notice describes:

- the uses and disclosures of PHI that may be made by the Plan;
- an individual's rights; and
- the Plan's legal duties with respect to the PHI.

The Notice informs individuals that the College will have access to PHI in connection with its plan administrative functions, including but not limited to payment and health care operations. The Notice also provides a description of the College's complaint procedures, the name and telephone number of the contact person for further information, and the effective date of the Notice.

The Notice will be individually delivered to all individuals:

- no later than April 14, 2004;
- on an on-going basis, at the time of an individual's enrollment in the Plan; and
- within 60 days after a material change to the notice.

2. Benefits Provided Through Insurance Policies

For group health benefits provided under a policy of insurance, the insurance company will develop and distribute a Notice of Privacy Practices describing how the insurance company will use and disclose medical information. The Notice of Privacy Practices prepared by the insurance company will govern the uses and disclosures of medical information by the insurance company.

E. Complaints

The Benefits and Compensation Manager, 100 East 8th Street, Suite 210, Holland, Michigan 49423 (616-395-7811) will be the Plan's contact person for receiving complaints. Complaints that are not resolved within 30 days by the Benefits and Compensation Manager may be appealed to the Privacy Officer. The Privacy Officer is responsible for enforcing the process for individuals to lodge complaints about the Plan's use and disclosure of PHI.

F. Sanctions for Violations of Privacy Policy

The Privacy Officer may apply sanctions (discipline) for using or disclosing PHI in violation of this Privacy Policy in accordance with the College's discipline policy, up to and including termination.

G. Mitigation of Inadvertent Disclosures of Protected Health Information

The College will mitigate, to the extent possible, any harmful effects that become known to it of a violation of this Privacy Policy. If an employee becomes aware of a disclosure of PHI that is not in compliance with this Privacy Policy, either by an employee of the Plan or an outside consultant or contractor, the employee must immediately contact the Privacy Officer so that the appropriate steps to mitigate harm to the individual can be taken.

H. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

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

I. Documentation

This Privacy Policy will be documented and maintained for at least six (6) years by the Privacy Officer. This Privacy Policy must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including changes and modifications in regulations). Any changes to this Privacy Policy must be promptly documented.

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

The Plan will document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights and maintain records, of such events for six (6) years. The documentation of any policies and procedures, actions, activities, and designations may be maintained in either written or electronic form.

III. POLICIES ON USE AND DISCLOSURE OF PHI

A. Access to PHI is Limited to Certain Employees

The following employees of the College ("employees with access") have access to PHI to perform administrative functions for the Plan. No other employees of the College are permitted to have access to PHI.

- Director of Human Resources.
- Benefits and Compensation Manager.

These employees 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 except to other employees with access, unless an authorization is in place or the disclosure otherwise is in compliance with this Privacy Policy. Employees who have access to PHI must comply with this Privacy Policy.

Employees with access may also perform duties for the employer that are not necessary for the administration of the Plan, collectively referred to as "employer functions." Some of these employer functions, such as administration of attendance, FMLA, worker's compensation and disability policies, may require the use of individually identifiable health information that is not PHI ("IIHI"). Employees with access will not use or consider PHI in the performance of any employer function unless pursuant to an authorization that specifically permits the disclosure of PHI to the College for that purpose. All IIHI collected for employer functions will be maintained separately from Plan files.

B. Use and Disclosure Defined

The College and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use*. The sharing, employment, application, utilization, examination, or analysis of PHI by any person working for or within the Human Resources Office of the College, 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 PHI to persons not employed by or working within the

Human Resources Office of the College and involved in the administration of the Plan.

C. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the Plan's own payment or health care operations. PHI may be disclosed to another covered entity or health insurance issuer that participates with the Plan in an organized healthcare arrangement for any health care operations activities of the arrangement. PHI may be disclosed to another covered entity for the payment purposes of that covered entity, or for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the covered employee and the PHI requested pertains to that relationship.

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes but is not limited to:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance), and related health care data processing.

Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration, including but not limited to:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development; and

- business management and general administrative activities.

D. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the College's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the covered employee has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

E. Mandatory Disclosures of PHI: to Individual and DHHS

An individual'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 (see the policy for "Access to Protected Information and Request for Amendment" that follows); and

- the disclosure is made to the U.S. Department of Health and Human Services or DHHS for purposes of enforcing HIPAA.

E. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without an individual's authorization, when specific requirements are satisfied, including prior approval of the Privacy Officer. Disclosures are permitted:

1. about victims of abuse, neglect, or domestic violence, if:

    - the individual agrees with the disclosure; or

    - the disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect, or violence.

2. for judicial and administrative proceedings in response to:

   - an order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); and

   - a subpoena, discovery request, or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.

3. for law enforcement purposes, if

   - pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information;

   - information requested is limited information needed to identify or locate a suspect, fugitive, material witness, or missing person;

   - information about a suspected victim of a crime (a) if the individual agrees to disclosure, or (b) without agreement from the individual, if the information is not to be used against the victim, if the need for information is urgent, and if disclosure is in the best interest of the individual;

   - information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct; or

   - information that constitutes evidence of criminal conduct that occurred on the College's premises.

4. for public health activities;

5. for health oversight activities;

6. to a coroner or medical examiner about decedents, for the purpose of identifying a deceased person, determining the cause of death, or other duties as authorized by law;

7. that relate to workers' compensation programs, to the extent necessary to comply with laws relating to workers' compensation or other similar programs; and

8. for other legal or Public Policy purposes authorized by the HIPAA Privacy Regulations, 45 C.F.R. §164.512.

F. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if our authorization form, or a form acceptable to us, is fully completed and signed by the individual or the individual's representative. A copy of the signed form will be returned to the individual after it is received by the Plan. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. Information disclosed pursuant to an authorization may be re-disclosed by the recipient and will no longer be subject to this Privacy Policy. The authorization may be revoked by writing to the Privacy Officer at any time, but revocation will not affect disclosures made prior to the revocation.

To be effective all information on the authorization must be completed. This includes specifically and meaningfully describing the information to be disclosed and the purpose of the disclosure, and identifying the persons authorized to disclose the PHI and the persons to whom disclosure may be made. The authorization must specify an expiration date or time period, and will not be used beyond that date. It must be signed and dated by the individual, or if signed by a representative of an individual, must include a statement describing the representative's authority to act for the individual. If payment, treatment or enrollment is conditioned upon receipt of the authorization, the form will state this.

G. Complying With the "Minimum-Necessary" Standard

Minimum Necessary When Disclosing and Requesting PHI. For making *disclosures* or *requests* for PHI to any party for any purpose, information must be the minimum necessary to accomplish the purpose of the disclosure.

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 a valid authorization;
- disclosures made to the DOL;
- uses or disclosures required by law;
- uses or disclosures required to comply with HIPAA; and

- disclosures made to a health are provider for treatment, payment, or health care operations.

H. Disclosures of PHI to Business Associates

Employees with access 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 with access must contact the Privacy Officer and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing a Plan function or activity involving the use or disclosure of protected health information (including claims processing or administration, data analysis, underwriting, 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.

I. Disclosures of De-Identified Information

The Plan may freely 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. The two ways a covered entity can de-identify information are by professional statistical analysis or by removing 18 specific identifiers specified in 45 C.F.R. §164.514.

J. Requests for Disclosure of PHI From Spouses, Family Members, and Friends

The Plan will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. The Plan may disclose a limited amount of PHI (excluding diagnosis) in an explanation of benefits as part of the Plan's payment functions.

PHI, including diagnosis, may be disclosed without an authorization if the spouse, family member, or personal friend is:

1. the parent of the individual and the individual is a minor child;

2. the personal representative of the individual, in which case the PHI may be released by following the procedure for "Verification of Identity of Those Requesting Protected Health Information"; or

3. the covered employee, and the individual participates in the Plan as the dependent of the covered employee, and the covered employee contacts the Plan to discuss payment related to the individual's health care. In this circumstance the Plan may reasonably infer that it is in the individual's best interest to allow the covered employee to act on behalf of the individual and the Plan may disclose PHI directly relevant to the covered employee's involvement with the individual's care or payment. The Plan will not disclose information to a non-employee spouse or parent who is not a personal representative of the individual.

An individual may revoke the Plan's authority to disclose PHI pursuant to 2. or 3. above by filing a written request for restriction of disclosure with the Plan. All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved pursuant to the procedures for "Disclosures Pursuant to Individual Authorization."

IV. POLICIES ON INDIVIDUAL RIGHTS

A. Access to Protected Health Information and Requests for Amendment

HIPAA gives individuals the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that individuals may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by individuals pursuant to the procedures specified in the Notice. The Privacy Officer may deny requests for documents that were compiled for a legal proceeding or information obtained under a promise of confidentiality.

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

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or

- other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

B. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI by submitting a written request to the Privacy Officer. This right to an accounting extends to disclosures made in the last six (6) years, other than disclosures:

- to carry out treatment, payment, or health care operations;
- to individuals about their own PHI;
- pursuant to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for other national security or law enforcement purposes.

The Plan will respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the individual notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period will be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.

C. Requests for Alternative Communication Means or Locations

Individuals may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, individuals may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the Privacy Officer, the requests are reasonable and do not impose an administrative burden on the Plan.

However, the Plan will accommodate reasonable requests for the communication of PHI by alternate means or at alternate locations if the individual clearly provides

information that the disclosure of all or part of that information could endanger the individual. The Privacy Officer has the responsibility for administering requests for confidential communications.

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

An individual may request restrictions on the use and disclosure of the individual's PHI. It is the Plan's policy to attempt to honor such a request only in rare and unusual circumstances and only if, in the sole discretion of the Privacy Officer, the request is reasonable. The Privacy Officer is responsible for administering requests for restrictions.

E. Verification of Identity of Those Requesting Protected Health Information

The identity of individuals who request access to PHI will be verified. The authority of any person requesting access to PHI will be verified if the identity or authority of such person is not known.

Request Made by Individual. When an individual requests access to his or her own PHI, the individual must present a valid driver's license, passport, or other photo identification issued by a government agency, which will be copied and filed with the individual's designated record set.

Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor child, the person's relationship with the child will be verified by confirming enrollment of the child in the parent's plan as a dependent, and the same identification procedure will be followed as for an individual request.

Request Made by Personal Representative. When a personal representative requests access to an individual's PHI, a copy of a valid power of attorney will be copied and filed with the individual's designated record set.

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 "Mandatory Disclosures of PHI," or "Permissive Disclosures of PHI," the following steps will be followed to verify the official's identity and authority:

- An agency identification badge, other official credentials, or other proof of government status will be copied and filed with the individual's designated record set.

- If the request is in writing, it will be verified that the request is on the appropriate government letterhead.

- If the request is by a person purporting to act on behalf of a public official, a written statement on appropriate government letterhead will be requested stating that the person is acting under the government's authority, or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

- A written statement of the legal *authority* under which the information is requested or, if a written statement would be impracticable, an oral statement of such legal authority will also be required. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the College's legal counsel.

V. EFFECTIVE DATE

The Privacy Policy is effective April 14, 2004.

This Privacy Policy is adopted this _____ day of _____, 2004.

Hope College Employee Benefit Plan
by and through its Plan Sponsor,
Hope College

By_____
Its Director of Human Resources