PRIVACY NOTICE

Notice of Health Information Practices

This notice describes how information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

The group healthcare plan collects the following types of information in order to provide benefits:

- Information that you provide to the plan to enroll in the plan, including personal information such as your address, telephone number, date of birth, and Social Security number.
- Plan contributions and account balance information.
- The fact that you are or have been enrolled in the plans.
- Health-related information received from any of your physicians or other healthcare providers.
- Information regarding your health status, including diagnosis and claims payment information.
- Changes in plan enrollment (e.g., adding a participant or dropping a participant, adding or dropping a benefit).
- Payment of plan benefits.
- Claims adjudication.
- Case or medical management.
- Other information about you that is necessary for us to provide you with health benefits.

Understanding Your Health Record/Information

Each time you visit a hospital, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment. This information, often referred to as your health or medical record, serves as a:

- Basis for planning your care and treatment.
- Means of communication among the many health professionals who contribute to your care.
- Legal document describing the care you received.
- Means by which you or a third-party payer can verify that services billed were actually provided.
- Tool in educating health professionals.
- Source of data for medical research.
- Source of information for public health officials charged with improving the health of the nation.
- Source of data for facility planning and marketing.
- Tool with which the University of Dayton can assess and continually work to improve the benefits offered by the group healthcare plan.

Understanding what is in your record and how your health information is used helps you to:

- Ensure its accuracy.
- Better understand who, what, when, where, and why others may access your health information.
- Make more informed decisions when authorizing disclosure to others.

Your Health Information Rights

Although your health record is the physical property of the plan, the healthcare practitioner, or the facility that compiled it, the information belongs to you. You have the right to:

- Request a restriction on otherwise permitted uses and disclosures of your information for treatment, payment, and healthcare operations purposes and disclosures to family members for care purposes.
- Obtain a paper copy of this notice of information practices upon request, even if you agreed to receive the notice electronically.
- Inspect and obtain a copy of your health records by making a written request to the plan privacy officer, John E. Hart, University Counsel or the Office of Human Resources.
- Amend your health record by making a written request to the plan privacy officer that includes a reason to support the request.
- Obtain an accounting of disclosures of your health information made during the previous six years by making a written request to the plan privacy officer or the Office of Human Resources.

- Request communications of your health information by alternative means or at alternative locations.
- Revoke your authorization to use or disclose health information except to the extent that action has already been taken.

Group Health Plan Responsibilities

The group healthcare plan is required to:

- Maintain the privacy of your health information.
- Provide you with this notice as to the plan's legal duties and privacy practices with respect to information that is collected and maintained about you.
- Abide by the terms of this notice.
- Notify you if the plan is unable to agree to a requested restriction.
- Accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations.

The plan will restrict access to personal information about you only to those individuals who need to know that information to manage the plan and its benefits. The plan will maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your personal information. Under the privacy standards, individuals with access to plan information are required to:

- Safeguard and secure the confidential personal financial information and health information as required by law. The plan will only use or disclose your confidential health information without your authorization for purposes of treatment, payment, or healthcare operations. The plan will only disclose your confidential health information to the University of Dayton for plan administration purposes.
- Limit the collection, disclosure, and use of participant's healthcare information to the minimum necessary to administer the plan.
- Permit only trained, authorized individuals to have access to confidential information.

Individuals who violate this policy will be subject to the University of Dayton's established disciplinary process.

Communication with family. Under the plan provisions, the University of Dayton may disclose to an employee's family member, guardian, or any other person you identify, health information relevant to that person's involvement in your obtaining healthcare benefits or payment related to your healthcare benefits.

Notification. The plan may use or disclose information to notify or assist in notifying a family member, personal representative, or another person responsible for your care, your location, general condition, plan benefits, or plan enrollment.

Business associates. There are some services provided to the plan through business associates. Examples include accountants, attorneys, actuaries, medical consultants, and financial consultants, as well as those who provide managed care, quality assurance, claims processing, claims auditing, claims monitoring, rehabilitation, and copy services. When these services are contracted, it may be necessary to disclose your health information to our business associates in order for them to perform the job we have asked them to do. To protect employees' health information, however, the University of Dayton will require the business associate to appropriately safeguard this information.

Benefit coordination. The plan may disclose health information to the extent authorized by and to the extent necessary to comply with plan benefit coordination.

Workers' compensation. The plan may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs established by law.

Law enforcement. The plan may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena.

The plan reserves the right to change its practices and to make the new provisions effective for all protected health information it maintains. Should the University of Dayton's information practices change, it will mail a revised notice to the address supplied by each employee.

The plan will not use or disclose employees' health information without their authorization, except as described in this notice.

For More Information or to Report a Problem

If you have questions and would like additional information, you may contact John E. Hart, University Counsel at (937) 229-4333 or the University Office of Human Resources at (937) 229-2541 or the Research Institute Office of Human Resources at (937) 229-2039.

If you believe your privacy rights have been violated, you can file a complaint with John E. Hart or with the Secretary of Health and Human Services. There will be no retaliation for filing a complaint.

The plan reserves the right to change the terms of this notice and to make the new notice provisions effective for all protected health information that it maintains. Any new notice will be sent to you by first-class mail or electronically if you so agree.

The effective date of this notice is April 14, 2003.

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

Name: _____

Health record number: _____

Date of birth:_____

1. I authorize the use or disclosure of the above named individual's health information as described below.
2. The following individual or organization is authorized to make the disclosure:

   _____

   Address: _____
3. The type and amount of information to be used or disclosed is as follows: (include dates where appropriate)

   ___ Enrollment

   ___ Payment

   ___ Claims adjudication

   ___ Case or medical management records including:

   __ Problem(s) [list] from (date) _____ to (date) _____

   __ Medication(s) [list] from (date) _____ to (date) _____

   __ Most recent history and physical

   __ Most recent discharge summary

   __ Laboratory results from (date) _____ to (date) _____

   __ X-ray and imaging reports from (date) _____ to (date) _____

   __ Consultation reports from (doctors' names) _____

   __ Entire record from (date) _____ to (date) _____

   Other_____
4. This information may be disclosed to and used by the following individual or organization:

   _____

   Address: _____ for the purpose of:_____
5. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization, I must do so in writing and present my written revocation to _____. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy. Unless otherwise revoked, this authorization will expire on the following date, event, or condition: _____.

   If no expiration date, event, or condition is specified, this authorization will expire in six months.
6. I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this authorization. I understand that I may inspect or copy the information to be used or disclosed. I understand that any disclosure of information carries with it the potential for an unauthorized redisclosure and the information may not be protected by federal confidentiality rules. If I have questions about disclosure of my health information, I can contact the University of Dayton Office of Human Resources at (937) 229-2541 or the Research Institute Office of Human Resources at (937) 229-2039.

   Signature of employee, plan participant, or legal representative:

   _____ Date _____

   If signed by legal representative, authority to act for employee/plan participant:

   _____

   _____

   Signature of witness:

   _____

PLAN AMENDMENTS

The University of Dayton's Anthem medical plans are subject to the Health Insurance Portability and Accountability Act (HIPAA). On the basis of that law, privacy regulations apply to certain protected health information. The following provisions are adopted to comply with those requirements:

The University of Dayton may only use and disclose protected health information for plan administrative functions that it performs for the plan. Information used and disclosed without specific authorization must be for treatment, payment, or healthcare operations.

The plan will not disclose protected health information to the University of Dayton unless and until it receives a certification from the University of Dayton that it agrees to:

1. Not use or disclose the information other than permitted by the plan document or required by law.
2. Ensure that any of its agents, including a subcontractor, to whom it provides protected health information agree to the same restrictions that apply to the University of Dayton with respect to such information.
3. Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the University of Dayton.
4. Report to the group health plan any use or disclosure of the information that is inconsistent with the permitted uses or disclosures provided for of which it becomes aware.
5. Provide an individual with access to inspect or to obtain a copy of the protected health information that the plan has about the individual upon request.
6. Make available protected health information for amendment and incorporate any required amendments to protected health information.
7. Make available the information required to provide an accounting of disclosures of protected health information about an individual.
8. Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary of the Department of Health and Human Services for purposes of determining compliance by the group health plan with this subpart.
9. If feasible, return or destroy all protected health information received from the group health plan that the University still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
10. Ensure that the adequate separation between the plan and the University of Dayton is established.

Separation between the plan and the University of Dayton must be maintained by the following:

1. Access to the protected health information to be disclosed is limited to the Director of Compensation & Benefits, the Benefits Manager, the Benefits Specialist, the HR Generalists and any other employee of Human Resources who has need to access the information for business purposes.
2. The access to and use of the protected health information by the employees and other persons described above is restricted to plan administrative functions that the University of Dayton performs for the plan.
3. Employees of other persons described above who violate the provisions of this plan document with respect to the regulations protecting the confidentiality of health information are subject to discipline including termination of employment under the Sanctions Policy of the plan and/or the University of Dayton.

PLAN SPONSOR CERTIFICATION

The plan sponsor of the group health plan, the University of Dayton, certifies that it will:

1. Not use or disclose the information other than permitted by the plan document or required by law.
2. Ensure that any of its agents, including a subcontractor, to whom it provides protected health information agree to the same restrictions that apply to the University of Dayton with respect to such information.
3. Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the University of Dayton.
4. Report to the group health plan any use or disclosure of the information that is inconsistent with the permitted uses or disclosures provided for of which it becomes aware.
5. Provide an individual with access to inspect or to obtain a copy of the protected health information that the plan has about the individual upon request.
6. Make available protected health information for amendment and incorporate any required amendments to protected health information.
7. Make available the information required to provide an accounting of disclosures of protected health information about an individual.
8. Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary of Health and Human Services for purposes of determining compliance by the group health plan with this subpart.
9. If feasible, return or destroy all protected health information received from the group health plan that the University of Dayton still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
10. Ensure that the adequate separation between the plan and the University of Dayton is established.

General HIPAA Health Information Privacy Policy

The University of Dayton sponsors a group healthcare plan that is subject to the Health Insurance Portability and Accountability Act (HIPAA). On the basis of that law, privacy regulations now apply to certain protected health information. The University of Dayton as plan sponsor has adopted the following policy to comply with these regulations. The University of Dayton's medical privacy policy will continue to apply to medical information, and the University of Dayton will comply with all other federal and state laws concerning medical privacy.

The University of Dayton generally only performs enrollment, changes in enrollment, and payroll deductions, and to the extent it obtains HIPAA-protected health information (PHI), it will maintain that information in confidence. Specifically, the University of Dayton will not use or disclose such information for employment-related actions and decisions or in connection with other benefit plans.

PHI refers to individually identifiable health information received by the University of Dayton's group health plan and created or received by a healthcare provider, health plan, or healthcare clearinghouse that relates to the past, present, or future health of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care. Such health information includes health status, medical condition, claims experience, receipt of health care, medical history, genetic information, and evidence of insurability and disability.

PHI does not refer to health information received apart from a group health plan, such as workers' compensation, short-term disability, long-term disability, medical information received based upon the Americans with Disabilities Act (ADA), medical information received based upon the Family and Medical Leave Act (FMLA), or preemployment physicals. However, the University of Dayton's medical privacy policy will apply to such information.

The plan and its insurers/HMOs will only disclose summary health information to the University of Dayton for the purpose of obtaining premium bids or for the purposes of modifying, amending, or terminating the Employment Retirement Income Security Act (ERISA) healthcare plan. The plan and its insurers/HMOs will not disclose PHI to the University of Dayton. As a plan sponsor, the University of Dayton will request summary health information only for the purpose of obtaining premium bids or for the purposes of modifying, amending, or terminating the ERISA healthcare plan. Summary health information means claims history, claims expenses, or type of claims experienced from which the following information has been deleted:

- Names
- Street address, city, county, ZIP code (except that geographic information may be aggregated by a five-digit ZIP code)
- All elements of dates (except year)
- Telephone numbers
- Fax numbers
- Electronic-mail addresses
- Social Security numbers
- Medical records 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 (URL)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Before assisting employees with understanding the group health plan, filing claims, or disputing claims, the University of Dayton will obtain an individual's authorization to access that person's protected health information.

The University of Dayton, as plan administrator and plan sponsor, will provide plan participants with a summary plan description. A notice of the privacy practices will be provided by the HMO or health insurer.

The University of Dayton will discipline (up to and including discharge) employees for improper access, use, or disclosure of protected health information or other confidential medical information.

The University of Dayton will not take any retaliatory action against any person for filing a complaint, assisting in an investigation, or otherwise opposing any act under the HIPAA privacy regulations.

Any protected health information will be secured against unauthorized access.

When protected health information is used for payment of benefits and plan operations, only the minimum necessary information will be released.

As plan sponsor, the University of Dayton will amend the plan to comply with the HIPAA privacy regulations. These amendments will include that:

- Certain classes of employees or others are granted access to PHI.
- Access to PHI will be only for the group healthcare plan administrative functions.
- The group healthcare plan will only permit the use and disclosure of PHI consistent with the HIPAA privacy regulations.
- Business associates of the plan or the University of Dayton will agree to comply with applicable HIPAA privacy regulations if they receive PHI.
- No PHI will be used in employment-related actions or in connection with any other employee benefit plan.
- PHI will be accessible to individuals, available for amendment, and available for an accounting for disclosures consistent with HIPAA privacy regulations. As the HIPAA privacy regulations change, the University of Dayton will amend the plan to comply with the changes.

As the plan sponsor, the University of Dayton will comply with the terms of the plan regarding the use of protected health information as required by HIPAA.

As the plan sponsor, the University of Dayton will:

- Make the required certifications as to its use of the PHI (including as plan sponsor).
- Not use the PHI for employment or other benefit-plan purposes.
- Assist in the implementation of the amendment, access, and accounting rights provided in the group health plan.
- Restrict access to PHI so that employees of the University of Dayton do not access PHI unless it is part of their job duties with respect to benefit management.
- Use the PHI only for plan administration purposes.

As the plan sponsor, the University of Dayton will require business associates (such as providers of claims processing, administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, legal, accounting, actuarial, or financial consulting) to comply with applicable provisions of HIPAA privacy regulations. These obligations include:

- Using or disclosing PHI only as necessary to perform its function
- Returning the PHI (where feasible) at the end of the contract
- Helping the plan and plan sponsor comply with privacy standards
- Binding any subcontractors with access to PHI to similar promises

Records regarding PHI disclosures will be maintained for six years as required by HIPAA privacy regulations.

All disclosures made by the group healthcare plan entity for the last six years, other than for treatment, payment, or healthcare operations, may be requested for an accounting by an individual group healthcare plan participant.

John E. Hart, University Counsel is designated as the privacy officer for compliance with the HIPAA privacy regulations.

Group healthcare plan participants have the right to access, inspect, and copy their PHI that is maintained by the plan in accordance with HIPAA privacy regulations.

Group healthcare plan participants have the right to request the amendment of PHI.

Group healthcare plan participants can request restrictions on the uses and disclosures of PHI; however, the plan can decline to comply with such requests.

Policy and Procedure: Privacy Rule Compliance

The plan will follow the federal HIPAA privacy regulations with respect to the confidentiality of health information records. The following rules, therefore, will govern the confidentiality of such records in the custody of the plan, plan administrator, and claims administrator:

Any information disclosed to the University of Dayton as a self-funder, plan administrator, or claims administrator that is HIPAA-protected health information (PHI) will be treated as "confidential." Access to PHI will be only for group healthcare plan administration functions, and PHI will be released only to the minimum extent necessary to carry out such functions as enrollment, changes in enrollment, payroll deductions, filing benefit claims, paying benefits, explanations of benefits, coordination of benefits, denial of benefits, etc. The plan will only permit the use and disclosure of PHI consistent with the HIPAA privacy regulations.

The members of the Human Resources staff whose jobs require work with the health and dental insurance plans may access HIPAA-protected health information (PHI).

Any information that is on file with either the University of Dayton, plan administrator, or the claims administrator shall be available to the participant, except as provided in the HIPAA privacy regulations.

Business associates of the plan or the plan sponsor (such as providers of claims processing, claims processing administration, data analysis, utilization review, quality assurance, billing, benefit management, or practice management; or legal, accounting, actuarial, or financial consulting) will be required to agree to comply with applicable HIPAA privacy regulations if they receive PHI.

The University of Dayton will not permit PHI to be used in employment-related actions or in connection with any other employee-benefit plan. Before any PHI is released to a plan sponsor or administrator who is also an employer, that entity will be required to agree that PHI will not be used in employment-related actions or in connection with any other employee-benefit plan, and to report any impermissible use or disclosure of PHI.

The participant may request that any PHI be corrected, amended, or deleted.

The participant may request an accounting of PHI disclosures.

The plan will issue a notice of privacy practices to participants.

The plan administrator is to designate a privacy officer to implement and enforce this policy, adopt additional policies and procedures consistent with this policy, adopt policies and procedures consistent with any future HIPAA privacy regulations, and train individuals to carry out these policies and procedures. Such policies and procedures shall include administrative, technical, and physical safeguards to protect the privacy of PHI. The privacy officer is responsible for receiving complaints regarding privacy practices and responding to questions concerning the notice of privacy practices.

Policy and Procedure: Minimum and Necessary Standard

The group health plan will only use and disclose the minimum necessary protected health information to accomplish the purpose that the information is being used or disclosed for. In addition, when requesting a disclosure of protected health information, the group health plan will only request the minimum necessary to accomplish the purpose that the information is requested for.

Except for uses and disclosures that are exempt from the minimum necessary requirement and routine requests and disclosures listed below, determinations of the minimum necessary amount of information to be requested or disclosed will be made by the "privacy officer" based on the facts and circumstances of each case. The decision of the privacy officer may be appealed under the health information privacy complaint procedure. In determining the minimum amount of information necessary for a particular purpose, the privacy officer may need only determine the minimum amount that is reasonably necessary and does not have to determine the absolute minimum necessary.

The following uses and disclosures are exempt from the minimum necessary requirement:

- Disclosures to or requests by providers for treatment
- Disclosures to the individual that is the subject of the information
- Disclosures made pursuant to an individual's authorization
- Disclosures to the U.S. Department of Health and Human Services for enforcement purposes
- Uses or disclosures required by law
- Use or disclosures required for compliance with HIPAA Administrative Simplification Rules

The following employees and classes of employees may only have access to the specified type of information:

Employee/Class of Employees	Type of information
Director of Compensation & Benefits	All participant and dependent identification
Benefits Manager	information, enrollment status and any claims
Benefits Specialist	information required to assist with claims
HR Generalists	processing problems.

Routine Disclosures

When a provider requests information about whether an individual is covered by the plan for purposes of filing a claim and provides the individual's membership number, disclosure of whether the individual is covered and the extent of the coverage provided is the minimum necessary information necessary and may be disclosed by the members of the Human Resources staff listed above without review by the privacy officer.

When a provider who has filed a claim requests information about the status of a claim, the claims administrator, disclosure that the claim has been decided or is pending is the minimum information necessary and may be disclosed by the claims administrator without review by the privacy officer. If the claim has already been decided, disclosure of the decision and the reason for the decision is the minimum information necessary and may be disclosed by the claims administrator without review by the privacy officer.

Policy and Procedure: Authorizations to Disclose Protected Health Information

Except where otherwise permitted, the group health plan will not request or disclose protected health information (PHI) without a valid authorization.

Protected health information may be disclosed without authorization:

- To the individual who is the subject of the information
- For treatment, payment, or healthcare operations
- Incident to a permitted or required disclosure as long as the minimum necessary and administrative, technical, and physical safeguards have been followed.
- Pursuant to an agreement with opportunity to agree or object for very limited information in certain limited circumstances.
- When required by law, for public health purposes, and similar purposes.
- To comply with workers' compensation and similar laws.

PHI must be disclosed to the individual when requested and during compliance investigations.

The plan Privacy Officer will determine if an authorization request directed to the group health plan meets the requirements of the HIPAA Privacy Rule.

A valid authorization must contain at least the following required elements:

- A specific and meaningful description of the information to be used or disclosed.
- The name or other specific identification of who is authorized to make the requested use or disclosure.
- The name or other specific identification of to whom the covered entity may make the disclosure.
- A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization.
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research.
- Signature of the individual and date.

Signed authorizations will be retained for six years following their expiration.

The authorization must contain statements to give the individual notice of all the following (if applicable):

- The right to revoke the authorization in writing.
- The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or a reference to the covered entity's privacy notice that includes this information.
- Whether treatment, payment, enrollment, or eligibility for benefits may or may not be conditioned on the authorization including the consequences of a refusal to sign the authorization when such a condition is allowed.
- The potential for information disclosed pursuant to the authorization to be redisclosed by the recipient and no longer be protected by the HIPAA Privacy Rule.

A signed copy of an authorization that was requested by the group health plan will be provided to the individual.

The individual generally will be allowed to revoke an authorization at any time, provided that the revocation is in writing unless the authorization was obtained as a condition of obtaining insurance coverage and the insurer has the legal right to contest a claim under the policy or to contest the policy itself.

Policy and Procedure: Administrative, Physical, and Technical Safeguards of PHI

The group health plan will provide administrative, physical, and technical safeguards for protected health information to prevent any intentional or unintentional use or disclosure in violation of the HIPAA Privacy Rule, the terms of the plan, and the plan's privacy policies. Safeguards will also be applied to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Access to protected health information is limited to employees whose job duties require such access. No other employees will be given keys and passwords allowing access to paper and electronic records that contain protected health information.

Paper records that contain protected health information will be kept in locked cabinets in a room that will be locked when not in use.

Access to electronic records that contain protected health information will be restricted and require a password.

A designated fax machine located in a limited-access area will be used for sending and receiving documents that include protected health information.

E-mails containing protected health information will be immediately filed in a secure area of the computer network and all other copies will be deleted.

Employees involved in discussions that include protected health information are to take reasonable measures to make sure that such discussions are not overheard.

Policy and Procedure: Distribution of the Privacy Notice

On or before April 14, 2003, the privacy notice required by the HIPAA Privacy Rule will be mailed by first class mail to all employees who are participants in the group health plan as of that date to their last known address. A copy of the notice and a log recording the names and addresses to which this privacy notice was mailed are to be maintained for six years after a revised notice is distributed. This notice is included in the medical plan certificates from Anthem.

The notice will be mailed to all employees who become covered by the group health plan after April 14, 2003, as soon as they become covered. A copy of the notice and a log documenting these mailings are to be maintained for six years after a revised notice is distributed.

The notice will be mailed to all nonemployees who elect coverage under COBRA. A copy of the notice and a log documenting these mailings are to be maintained for six years after a revised notice is distributed.

The notice will be revised each time there is a material change in the required contents including a change in the law, regulations, or the policies of the group health plan. A revised notice will be sent to all employees who are participants in the group health plan at the time of the notice revision within 60 days of the revision. A copy of the revised notice and a log of the names and addresses to which the revised notice was mailed are to be maintained for six years after another revised notice is distributed.

At least once every three years, the health plan will notify all employees covered by the plan of the availability of the notice and how to obtain the notice. A copy of this notice and a log documenting the mailing are to be maintained for six years after the next notice of availability is distributed.

The privacy notice is to be prominently posted on the group health plan customer service website.

The plan privacy officer, or designee will prepare a privacy notice that meets the requirements of the HIPAA Privacy Rule. The privacy officer or designee will distribute a copy of the notice to any individual covered under the plan upon request. A record of each such distribution shall be maintained for six years.

The notice will be provided by e-mail to any employees who agree to receive the notice by e-mail. An employee's agreement to receive the notice by e-mail may be withdrawn at any time. A paper copy of the notice will be mailed if the plan knows that the e-mail transmission has failed. An employee who receives an e-mail notice may request a paper copy. A record of all agreements to receive the notice by e-mail must be retained for six years after they are no longer in effect. A record of all e-mail notice transmissions is to be retained for six years after a revised e-mail notice is distributed.

The plan privacy officer is responsible for preparing and distributing the privacy notice. All requests for copies of the privacy notice are to be directed to the Office of Human Resources.

Policy and Procedure: Requests for Access to PHI

The group health plan will provide individuals with access to inspect and obtain a copy of protected health information about the individual that the group health plan has in its records within 30 days of such a request. If necessary, the plan may extend this deadline by 30 days in a written statement to the individual that explains the reasons for the delay and the expected date of completion of the request.

If the request for access is for protected health information that is not maintained or accessible by the plan on-site, the plan will provide access within 60 days of the request. If necessary, the plan may extend this deadline by 30 days in a written statement to the individual that explains the reasons for the delay and the expected date of completion of the request.

Requests for access are to be made in writing to the privacy officer. This requirement is to be specified in the plan's privacy notice.

The access is to be provided in the form or format requested by the individual, if it is readily producible, or, if not, in a readable hard copy form or such other form or format that is agreed to.

If the individual so agrees in advance to receive a summary or explanation of the requested information and agrees in advance to the fees that will be charged for the summary or explanation, the plan may provide the individual with a summary of the protected health information requested or an explanation of the protected health information requested.

A convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request is to be arranged.

Reasonable cost-based fees may be charged for the supplies and labor of copying, for requested postage, and for preparing an explanation or summary of the protected health information.

The privacy officer may deny an individual access to protected health information without providing the individual an opportunity for review, if the protected health information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

The privacy officer may deny an individual access to protected health information provided the individual is given a right to have such denials reviewed in the following circumstances:

1. -A licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
2. -The protected health information makes reference to another person (other than a healthcare provider) and a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
3. -The request for access is made by the individual's personal representative and a licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

A denial is to be in writing and state the basis for the denial and explain the individual's right to a review of the denial and how to make a complaint under the plan's complaint procedure.

The review of any such denial will be performed by a licensed healthcare professional designated by the plan who did not participate in the original decision.

Policy and Procedure: Requests for Amendment of Protected Health Information

An individual may request that the group health plan amend protected health information about the individual. The plan may deny such a request, if it determines that the protected health information that is the subject of the request was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment, is not in the plan's records, would not be available to the individual for inspection under the Policy and Procedure for Access to Protected Health Information, or is accurate and complete.

Requests for amendments must be made in writing and include a reason to support the request.

The plan will respond to an amendment request no later than 60 days after receipt of the request by granting the request in whole or in part or denying the request in whole or in part. Any denial must be in writing.

If necessary, the plan may extend this deadline by 30 days in a written statement to the individual that explains the reasons for the delay and the expected date of completion of the request.

If the request is granted, the records that are subject to amendment must, at a minimum, be so identified with the amendment or a link to the amendment appended. The individual will be informed that the amendment is accepted, and the individual's identification of and agreement to have the plan notify the relevant persons with which the amendment needs to be shared will be obtained. The plan will make reasonable efforts to inform and provide the amendment within a reasonable time to the persons identified by the individual as having received protected health information about the individual and needing the amendment and to persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment, and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

If the plan denies the requested amendment, in whole or in part, the plan will provide the individual with a timely, written denial. The denial will be in plain language and contain the basis for the denial, the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement, a statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment, and a description of how the individual may complain pursuant to the plan's complaint procedures or to the Secretary of Health and Human Services. The name, or title, and telephone number of the contact person or office designated to receive complaints must be included.

The plan will permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The plan may reasonably limit the length of a statement of disagreement.

The covered entity may prepare a written rebuttal to the individual's statement of disagreement. If a rebuttal is prepared, the plan will provide a copy to the individual who submitted the statement of disagreement.

The plan will identify the protected health information that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the information.

If a statement of disagreement has been submitted by the individual, the plan will include the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, or an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

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

If the standard transaction form for a transmittal of the information does not permit the appended information to be included, the covered entity may separately transmit that material to the recipient of the standard transaction.

If the plan is informed by another HIPAA Privacy Rule covered entity that an individual's protected health information has been amended, the plan will amend the protected health information as described above.

The plan will document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation until six years after those designations are no longer in effect.

Policy and Procedure: Documentation of Privacy Decisions

The group health plan will maintain its policies and procedures, required communications, and records of any required action, activity, and designation in written and electronic form.

Written and electronic records will be maintained of the following if applicable:

- The designation of an affiliated covered entity.
- Any signed authorization.
- Copies of the privacy notice.
- Any agreement with an individual to restrict otherwise permitted uses and disclosures.
- The designated record sets that are subject to access by individuals.
- The titles of the persons or offices responsible for receiving and processing requests for access by individuals.
- The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.
- The information required to be included in a requested accounting of disclosures of protected health information, the written accountings provided to individuals requesting an accounting of disclosures of protected health information, and the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.
- The designation of a privacy official who is responsible for the development and implementation of the policies and procedures of the group health plan.
- The designation of a contact person or office who is responsible for receiving complaints and who is able to provide further information about matters covered by the privacy notice.
- Records of the training of employees on health information privacy requirements.
- All complaints received, and their disposition.
- All sanctions taken against employees for health information privacy violations.
- Revisions to health information privacy policies and procedures.

A required document must be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

Miscellaneous Policies and Procedures

Policy and Procedure: Training of Employees

All employees of the plan sponsor who perform work for the group health plan are to be trained so that they understand and are able to comply with the plan's policies and procedures with reference to protected health information by April 14, 2003. Any employee who begins performing work for the group health plan will be receive such training as soon as possible but no later than one month after beginning such work for the group health plan.

The plan privacy officer is responsible for providing and documenting the required training.

Policy and Procedure: Verifying the Identity of an Individual or Entity Requesting PHI

The identity of an individual requesting protected health information from the group health plan who is not known by the plan must be verified before the information is disclosed. The individual's authority to receive the information must also be verified. This requirement does not apply to information that is disclosed pursuant to an agreement with opportunity for the subject to agree or object.

The privacy officer or his/her designee will determine if any required identity document or statement is sufficient. If the circumstances are reasonable, the privacy officer or his/her designee may rely on statements and documents that on their face meet the requirements.

Policy and Procedure: Recognizing a Personal Representative

The group health plan will treat a personal representative as the individual for purposes of exercising health information privacy rights.

If, under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, the plan will treat such person as a personal representative.

If, under applicable law, a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative.

If, under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, the group health plan will treat such person as a personal representative.

Policy and Procedure: Complaints

Complaints about the group health plan's compliance with the requirements of the HIPAA Privacy Rule or the group health plan's health information privacy policies are to be delivered to the privacy officer at 300 College Park Dr., Dayton, OH 45469-1660. This information is to be included in the privacy notice.

The privacy officer will determine if a violation has occurred, take steps to mitigate any damage that has occurred, and discipline any employee who has violated the rule or plan policies.

Complaints that the privacy officer has violated the requirements of the HIPAA Privacy Rule or the group health plan's health information privacy policies are to be referred to the health benefits manager for resolution.

The privacy officer will keep a record of all filed complaints and their disposition for six years following the disposition of the complaint.

Policy and Procedure: Sanctions

The group health plan will discipline members of its workforce who fail to comply with the requirements of the HIPAA Privacy Rule or the group health plan's health information privacy policies.

The privacy officer is responsible for receiving complaints concerning employees' violations and monitoring employees to determine if violations have occurred. Discipline will be applied under the group health plan sponsor's disciplinary policy as outlined in the Employee Handbook.

This internal sanction policy does not apply to violations that are disclosures by whistleblowers and workforce member crime victims and in the case of retaliatory or intimidating actions taken against individuals for asserting their privacy rights. Complaints about these actions should be directed to the Department of Health and Human Services Office of Civil Rights.

The privacy officer will keep a record of all disciplinary actions taken for six years following the action.

Policy and Procedure: Mitigation of Violations

The group health plan will take all practical steps to reduce the harmful effects caused by uses or disclosures of protected health information in violation of its policies or procedures and the HIPAA Privacy Rule.

As soon as it learns about such a violation by the plan or its business associates, the plan privacy officer will halt the use or disclosure and seek the return or destruction of any documents or other information that was disclosed.

Policy and Procedure: Refraining from Intimidating or Retaliatory Acts

The group health plan will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

- An individual about whom the plan has protected health information for exercising his or her health information privacy rights or filing a complaint under the plan's complaint procedure.
- Anyone for filing a complaint about a health information privacy violation with the Department of Health and Human Services; testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing into such a violation; or opposing any act or practice made unlawful by the HIPAA Privacy Rule. To be covered by this protection, opposition to an unlawful act must be based on a good-faith belief that the practice opposed is unlawful, must be reasonable, and must not involve a prohibited disclosure of protected health information.

Policy and Procedure: Bar on Waivers of Privacy Rights by Individuals

The group health plan will not require individuals to waive their health information privacy rights or their right to file a complaint about a health information privacy violation with the Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.