HIPAA PRIVACY PROTECTIONS

HIPAA and the standards for Privacy of Individually Identifiable Health Information issued by the United States Department of Health and Human Services (the "Privacy Rule") require the Plan to protect the confidentiality of Protected Health Information that it obtains about Plan participants in the course of providing Plan health care benefits. The Privacy Rule applies to the health benefit programs. The Plan also requires its service providers (known as "Business Associates") that create, receive, or maintain your Protected Health Information to protect your Protected Health Information.

Under the Privacy Rule, the Plan may use and disclose your Protected Health Information as permitted or required by the Privacy Rule, as described in this document, or when you authorize the use or disclosure. Protected Health Information ("PHI") includes any information, whether oral or recorded, in any form or medium that is created or received by the Plan that relates to your past, present or future physical or mental health, including the provision of and payment for care, that identifies you or provides a reasonable basis for your identification. PHI does not include de-identified health information or health information that the University is entitled to under applicable law (for example, the FMLA, the Americans with Disabilities Act, the Occupational Safety and Health Act, workers' compensation laws, and other state and federal laws), or health information that the University obtains through sources other than the Plan and retains as part of your employment records (for example, drug screening tests, fitness for duty examination results or other types of similar information). This type of information, therefore, is not subject to the Privacy Rule, nor the restrictions described in this document.

As part of its efforts to comply with the HIPAA Privacy Rule, the Plan has appointed a Privacy officer. The Acting Privacy Officer for the Plan is:

Amy A. Rodriguez
Office of the General Counsel
656 W. Kirby, 4249 FAB
Wayne State University
Detroit, MI 48202
313-577-2268

The Privacy Officer is the person with whom you should lodge any complaints if you believe that the confidentiality of your or your covered dependents' PHI has been compromised in the course of administering the Plan's health benefit programs.

Required Disclosures of PHI by the Plan

The Plan must disclose your PHI:

- to you, with respect to your own PHI;
- to the Secretary of the United States Department of Health and Human Services to determine whether the Plan is in compliance with the Privacy Rule; or
- where required by law (this means that the Plan will make the disclosure only when the law requires it to do so, but not if the law would just allow it to do so.

Permitted Uses and Disclosures of PHI by the Plan

The Plan may use or disclose your PHI as necessary for the operation of the Plan as described in this document and under the following conditions:

- for treatment purposes, when necessary;
- to carry out Payment and Health Care Operations (as defined in the Privacy Rule);
- to the Plan's Workforce;
- to Business Associates that enter into Business Associate agreements with the Plan;
- under certain circumstances expressly permitted by the Privacy Rule;
- to you about treatment alternatives or other health-related benefits or services that may be of interest to you; or
- pursuant to a proper authorization received from you.

Even if a use or disclosure of PHI is permitted above, the Plan will comply with any special protections under state or federal law that are more protective of your privacy.

Uses and Disclosures of PHI Expressly Permitted by the Privacy Rule

The Plan may use or disclose your PHI as follows:

- as permitted by law (i.e. a state or federal law permits, but does not require, the Plan to make the disclosure);
- for public health purposes;
- to report information about victims of abuse, neglect or domestic violence;
- for health oversight activities;
- for judicial and administrative proceedings pursuant to judicial or administrative orders or where the Plan has received adequate assurances (as provided in the Privacy Rule), that the PHI to be disclosed will remain confidential;
- to your personal representative, after receiving proof that he or she may act on your behalf;
- to individuals involved with your care or payment for your care, if the Plan provides you with the opportunity to object and you do not, or the Plan infers from the circumstances that you do not object;
- for certain law enforcement purposes as set forth in the Privacy Rule;
- to correctional facilities regarding inmates;
- to report information about decedents to funeral directors, coroners and medical examiners;
- for purposes of cadaveric organ, eye or tissue donation;
- for use in a limited data set for purposes of research, public health or Health Care Operations, if a data use agreement has been signed;
- for research purposes;
- to avert a serious threat to health or safety;
- for emergencies and disaster relief;
- for specialized governmental functions (for example, national security or defense);
- incidental disclosures, provided the Plan puts reasonable physical safeguards in place; and

- for workers' compensation.

Disclosures of PHI by the Plan to the University

The Plan may disclose your PHI to the University to carry out Plan administrative functions because the University agrees to the following provision. These disclosures, however, will only be made to the Plan's Workforce. The University agrees to:

- not use or further disclose the information other than as permitted or required as explained in this document, or as required by law;
- ensure that any agents, including a subcontractor to whom it provides PHI received from the Plan, agree to the same restrictions and conditions that apply to the University with respect to such information;
- 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, except the University may make disclosures with respect to workers' compensation as described above;
- report to the Plan any use or disclosure of the PHI that is inconsistent with the uses or disclosures provided under the Plan of which it becomes aware;
- follow our University's reporting requirements whenever a potential breach of PHI occurs or is discovered;
- make available to you your PHI that is maintained by the Plan and provide you with the right to obtain a copy of your PHI disclosed to and retained by the University;
- permit you to amend your PHI maintained by the Plan and incorporate these amendments as required by the Privacy Rule;
- permit you to have an accounting of the disclosures of your PHI made by the Plan, as described in the following section titled, "Your Rights Under HIPAA and the Privacy Rule";
- make it internal practices, books and records relating to the use and disclosure of PHI received from the Plan available to the United States Department of Health and Human Services for purposes of determining compliance with the Privacy Rule;
- if feasible, return or destroy all PHI received from the 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; and
- ensure that adequate separation between the Plan and the University is established as described below.

The Plan and the University will take the steps to provide for the adequate separation between the Plan and the University. Only those employees of the University identified below as the Plan's Workforce will have access to your PHI. The Plan's Workforce will receive PHI, as needed in the ordinary course of business, to carry out the Payment, Health Care Operations or other functions necessary for the proper operation of the Plan. The Plan will restrict the access to, and use and disclosure of, your PHI by these employees to those administrative functions that the University performs for the Plan. The Plan may also disclose limited health information to the Plan's Workforce in connection with enrollment or disenrollment of individuals into or out of the Plan. The University will handle any complaint relating to non-compliance by addressing that issue with the employee. The University will also provide a

mechanism for resolving issues of noncompliance, including disciplinary action up to and including discharge.

The following employees are responsible for carrying out Plan administrative functions on behalf of the University and are entitled to receive and create PHI about you and your covered dependents in the course of carrying out their administrative duties for the Plan ("Plan's Workforce"):

- The Plan's Privacy Officer
- University Human Resources employees

To maintain the confidentiality of your PHI, you should only communicate with one of these individuals if you wish to inquire about any aspect of the Plan, a benefit claim, your entitlement to coverage or any other matter regarding the Plan's benefit programs that offer health care benefits.

The Plan's Workforce has been trained to protect any PHI communicated to them by you, your close family members, your health care provider, an insurer, an HMO, or any entity that has been engaged to carry out any activities on their behalf with respect to the payment of your covered benefits. Specifically, any PHI that these individuals may learn about you or your family in the course of administering the Plan will not be provided to the University for any employment-related purpose or for the administration of any other benefit programs sponsored and maintained by the University, without your express authorization.

Your Rights Under HIPAA and the Privacy Rule

You have certain rights, under HIPAA and the Privacy Rule, relating to your PHI maintained by the Plan. All requests to exercise your individual rights must be made in writing to the Privacy Officer. The Plan's insurers or HMOs keep their own records and you must make any requests relating to your PHI in those records directly to the insurer or HMO. The Plan's Notice of Privacy Practices that was provided to you contains a more detailed description of the Plan's privacy procedures and your rights under HIPAA.

Your rights include:

- **Right to Notice.** You have the right to receive a copy of the Plan's Notice of Privacy Practices. Contact Human Resources for a copy of the Notice.

- **Right to Access.** You have the right to access your PHI that is maintained by the Plan (or an insurer or HMO providing benefits under the Plan), so long as the information is retained in the Plan's medical, billing and claim adjudication (the "designated record set"). Requests for access to this information maintained by an insurer or HMO providing benefits under the Plan should be made directly to the appropriate insurer or HMO. The Plan (or an insurer or HMO) may charge a reasonable fee for copying the information you request, and the cost of any mailing. The Plan may deny your request for access, and, in certain circumstances, that decision will not be subject to review; while, in other circumstances, you may seek a review of the Plan's denial. In either case, if your request is denied, the Plan will respond in writing, explaining its reasons for the denial, whether the reason is reviewable, and the procedures for seeking review, if applicable. Any review will be conducted by someone designated by the Plan who was not involved in the original decision.

- **Right to an Accounting.** Within a single 12-month period, you may request one accounting of disclosures of your PHI made by the Plan at no charge. If you request more than one accounting within the same 12-month period, the Plan may charge you a reasonable fee. You will be

informed in advance of the proposed fee and will have an opportunity to revise or withdraw your request in order to avoid or reduce the fee. The Plan is obligated to provide you with an accounting of any disclosures of your PHI made within the 6-year period immediately prior to the date of your request, except disclosures made:

- for purposes of treatment, payment or healthcare operations;
- directly to you or close family members involved in your care;
- for purposes of national security;
- incidental disclosures (as defined in the Privacy Rule);
- a part of a limited data set (as defined in the Privacy Rule);
- to correctional institutions or law enforcement officials; and
- pursuant to your express authorization.

Requests for an accounting of disclosures from an insurer or HMO providing benefits under the Plan should be addressed to the appropriate insurer or HMO.

- **Right to Amend.** You may request that your PHI maintained in the records of the Plan be amended. When requesting an amendment, you are also required to state the basis or reason why you believe that the existing information is in error and needs to be revised. The Plan need not agree to your request.

  If your request is granted, the Plan will inform you of what changes or corrections it is making and how that will be done. If your request is denied, the Plan will provide you with:

  - the reasons for the denial;
  - an explanation of your right to submit a statement of disagreement and directions about how to do that;
  - a statement that even if you do not choose to submit a statement of disagreement, you may ask that your request for an amendment and the Plan's denial be provided with any future disclosures of the PHI that was the subject of your request; and
  - a description of the Plan's complaint procedures, including the name, address and phone number of the person with whom any complaint should be lodged. If you elect to submit a statement of disagreement, the Plan may submit a rebuttal statement in response. If the Plan chooses to submit a rebuttal statement, it will provide you with a copy.

  If the PHI that you are seeking to amend is not in the possession of the Plan, but is maintained by an insurer or HMO providing Plan benefits, the Plan will so inform you so that you may direct your request for an amendment directly to the insurer or HMO.

- **Right to Request Restrictions.** You may also request that the Plan restrict its uses and disclosures of your PHI for purposes which would otherwise be permissible under the HIPAA and the Privacy Rule. The Plan Administrator, or the appropriate Claims Administrator, need not agree to any restriction that you may request, but if it does agree to your request, the Plan will be bound to honor the restriction, until you indicate in writing that you are withdrawing the restriction, or the Plan or Claims Administrator informs you that it is withdrawing its consent to the restriction for a permitted reason under the Privacy Rule. The Plan's withdrawal of consent, however, will only apply to PHI created or received after you have been notified of the withdrawal of consent.

- **Right to Request Confidential Communications.** You may also request that the Plan communicate with you in a confidential manner, for example, by sending information to an

alternative address. The Plan will accommodate any reasonable request, though it will require that any alternative used still allow for payment information to be effectively communicated and for payments to be made. Requests for confidential communications made to the Plan Administrator will not bind any insurers or HMOs providing benefits under the Plan. If you wish that communications from insurers or HMOs be confidential, you must address those requests directly with the appropriate entity.

- **Right to File a Complaint.** If you believe your rights have been violated, you also have a right to file a complaint with the Plan's Privacy Officer or with the Secretary of the United States' Department of Health and Human Services. If you have questions about the status of your PHI or what is being done to protect its confidentiality, or if you wish to file a complaint, contact the Privacy Officer.

HIPAA SECURITY RULE

Effective as of April 20, 2005, HIPAA and the Standards for Security of Electronic Protected Health Information (the "Security Rule") require health plans to protect the confidentiality, integrity, and availability of your Electronic PHI ("EPHI") that they create, receive, transmit, or maintain about you in the course of providing health care benefits. To ensure the security of your EPHI, the University will comply with the Security Rule as set out below. The Plan has also required its Business Associates to agree to protect your EPHI.

EPHI includes any PHI that is transmitted or maintained in an Electronic Medium. "Electronic Medium" includes media used to store EPHI such as a hard drive computer, as well as media used to transmit your EPHI; for example, the Internet. The Security Rule does not cover PHI that began or was originally created in Electronic Media before being electronically transmitted. For example, EPHI transmitted paper-to-paper, fax-to-fax, by message containing EPHI left on voice-mail, through telephone calls, or by video conferencing is not covered by the Security Rule.

Disclosures of EPHI Expressly Permitted by the Security Rule

The Security Rule permits the Plan to disclose your EPHI to the University as follows:

- de-identified health information to the University, if the University requests the information for the purpose of obtaining premium bids from health plans for providing health insurance coverage under the Plan;
- de-identified health information to the University, if the University requests the information for the purpose of modifying, amending, or termination of the Plan;
- to the University when you authorize the disclosure; and
- to the University to determine your enrollment or eligibility status in the Plan.

Disclosures of EPHI by the Plan to the University

The Plan may disclose your EPHI to the University to carry out Plan administrative functions because the University agrees to the following provisions. These disclosures, however, will only be made to the Plan's Workforce. The University agrees to:

- implement "Policies and Procedures" that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of the Plan;
- make any documentation related to the Policies and Procedures available to the Secretary of the United States Department of Health and Human Services for the purpose of determining the Plan's compliance with the Security Rule;
- ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate security measures to protect the EPHI;
- report to the Plan any "Security Incident" of which it becomes aware, including an attempted or successful unauthorized access, use, disclosure, modification, or destruction of EPHI; and
- ensure that adequate separation between the Plan and the University is established and described below.

The Plan and the University will take steps to provide for the adequate separation between the Plan and the University for purposes of exposure to EPHI. Only members of the Plan's Workforce will have access to your EPHI.