AVE MARIA UNIVERSITY
HIPAA PRIVACY NOTICE

This Notice of Privacy Practices describes the legal obligations of Ave Maria University, Inc. (the "plan") and your legal rights regarding your protected health information held by the Plan under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

This Notice describes how the Plan uses and discloses the individual's personal health information. It also describes certain rights the individual has regarding this information. Additional copies of our Notice of Privacy Practices are available by calling Kathy Phelps, the Ave Maria University Director of Human Resources and Privacy Officer at 239-304-7074.

Definitions

- **Breach** means an unauthorized acquisition, access, use or disclosure of Protected Health Information ("PHI") or Electronic Protected Health Information ("ePHI") that violates the HIPAA Privacy Rule and that compromises the security or privacy of the information.
- **Protected Health Information** ("PHI") means individually identifiable health information, as defined by HIPAA, that is created or received by the Plan and that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information of persons living or deceased.

Commitment to Protecting Health Information

The Plan will comply with the Standards for Privacy of Individually Identifiable Health Information (i.e., the "Privacy Rule") set forth by the U.S. Department of Health and Human Services ("HHS") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Such standards control the dissemination of "protected health information" ("PHI") of Participants. Privacy Standards will be implemented and enforced in the offices of the Employer and Plan Sponsor and any other entity that may assist in the operation of the Plan.

The Plan is required by law to take reasonable steps to ensure the privacy of the Participant's PHI, and inform him/her about:

1. The Plan's disclosures and uses of PHI;
2. The Participant's privacy rights with respect to his/her PHI;
3. The Plan's duties with respect to his/her PHI;
4. The Participant's right to file a complaint with the Plan and with the Secretary of HHS; and
5. The person or office to contact for further information about the Plan's privacy practices.

Within this provision capitalized terms may be used, but not otherwise defined. These terms shall have the same meaning as those terms set forth in 45 CFR sections 160.103 and 164.501. Any HIPAA regulation modifications altering a defined HIPAA term or regulatory citation shall be deemed incorporated into this provision.

How Health Information May be Used and Disclosed

In general, the Privacy Rules permit the Plan to use and disclose, the minimum necessary amount, an individual's PHI, without obtaining authorization, only if the use or disclosure is:

1. To carry out Payment of benefits;
2. For Health Care Operations;
3. For Treatment purposes; or
4. If the use or disclosure falls within one of the limited circumstances described in the rules (e.g., the disclosure is required by law or for public health activities).

Disclosure of PHI to the Plan Sponsor for Plan Administration Purposes

In order that the Plan Sponsor may receive and use PHI for plan administration purposes, the Plan Sponsor agrees to:

1. Not use or further disclose PHI other than as permitted or required by the Plan documents or as required by law (as defined in the Privacy Standards);
2. Ensure that any agents, including a subcontractor, to whom the Plan Sponsor provides PHI received from the Plan, agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to such PHI;
3. Establish safeguards for information, including security systems for data processing and storage;
4. Maintain the confidentiality of all PHI, unless an individual gives specific consent or authorization to disclose such data or unless the data is used for health care payment or Plan operations;
5. Receive PHI, in the absence of an individual's express authorization, only to carry out Plan administration functions;
6. Not use or disclose genetic information for underwriting purposes;
7. Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or Employee benefit plan of the Plan Sponsor, except pursuant to an authorization which meets the requirements of the Privacy Standards;
8. Report to the Plan any PHI use or disclosure that is inconsistent with the uses or disclosures provided for of which the Plan Sponsor becomes aware;
9. Make available PHI in accordance with section 164.524 of the Privacy Standards (45 CFR 164.524);
10. Make available PHI for amendment and incorporate any amendments to PHI in accordance with section 164.526 of the Privacy Standards (45 CFR 164.526);
11. Make available the information required to provide an accounting of disclosures in accordance with section 164.528 of the Privacy Standards (45 CFR 164.528);
12. Make its internal practices, books and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of the U.S. Department of Health and Human Services ("HHS"), or any other officer or Employee of HHS to whom the authority involved has been delegated, for purposes of determining compliance by the Plan with part 164, subpart E, of the Privacy Standards (45 CFR 164.500 et seq);
13. Report to the Plan any inconsistent uses or disclosures of PHI of which the Plan Sponsor becomes aware;
14. Train Employees in privacy protection requirements and appoint a privacy compliance coordinator responsible for such protections;
15. If feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of such PHI 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 PHI infeasible; and

16. Ensure that adequate separation between the Plan and the Plan Sponsor, as required in section 164.504(f)(2)(iii) of the Privacy Standards (45 CFR 164.504(f)(2)(iii)), is established as follows:
    a. Privacy Officer: Is an Employee, or class of Employees, or other persons under control of the Plan Sponsor, who shall be given access to the PHI to be disclosed. The access to and use of PHI by the individuals described above shall be restricted to the plan administration functions that the Plan Sponsor performs for the Plan.
    b. In the event any of the individuals described above do not comply with the provisions of the Plan documents relating to use and disclosure of PHI, the Plan Administrator shall impose reasonable sanctions as necessary, in its discretion, to ensure that no further non-compliance occurs. The Plan Administrator will promptly report such violation or noncompliance to the Plan, and will cooperate with the Plan to correct violation or noncompliance to impose appropriate disciplinary action or sanctions. Such sanctions shall be imposed progressively (for example, an oral warning, a written warning, time off without pay and termination), if appropriate, and shall be imposed so that they are commensurate with the severity of the violation.

Disclosure of Summary Health Information to the Plan Sponsor

The Plan may disclose PHI to the Plan Sponsor of the group health plan for purposes of plan administration or pursuant to an authorization request signed by the Participant. The Plan may use or disclose "summary health information" to the Plan Sponsor for obtaining premium bids or modifying, amending, or terminating the group health plan.

Disclosure of Certain Enrollment Information to the Plan Sponsor

Pursuant to section 164.504(f)(1)(iii) of the Privacy Standards (45 CFR 164.504(f)(1)(iii)), the Plan may disclose to the Plan Sponsor information on whether an individual is participating in the Plan or is enrolled in or has un-enrolled from a health insurance issuer or health maintenance organization offered by the Plan to the Plan Sponsor.

Disclosure of PHI to Obtain Stop-loss or Excess Loss Coverage

The Plan Sponsor may hereby authorize and direct the Plan, through the Plan Administrator or the Claims Administrator, to disclose PHI to stop-loss carriers, excess loss carriers or managing general underwriters ("MGUs") for underwriting and other purposes in order to obtain and maintain stop-loss or excess loss coverage related to benefit claims under the Plan. Such disclosures shall be made in accordance with the Privacy Standards.

Other Disclosures and Uses of PHI:

Primary Uses and Disclosures of PHI

1. Treatment, Payment and Health Care Operations: The Plan has the right to use and disclose a Participant's PHI for all activities as included within the definitions of Treatment, Payment, and Health Care Operations and pursuant to the HIPAA Privacy Rule;
2. Business Associates: The Plan contracts with individuals and entities (Business Associates) to perform various functions on its behalf. In performance of these functions or to provide services, Business Associates will receive, create, maintain, use or disclose PHI, but only after the Plan and the Business Associate agree in writing to contract terms requiring the Business Associate to appropriately safeguard the Participants, information; and
3. Other Covered Entities: The Plan may disclose PHI to assist health care Providers in connection with their treatment or payment activities or to assist other covered entities in connection with payment activities and certain health care operations. For example, the Plan may disclose PHI to a health care Provider when needed by the Provider to render treatment to a Participant, and the Plan may disclose PHI to another covered entity to conduct health care operations. The Plan

may also disclose or share PHI with other insurance carriers (such as Medicare, etc.) in order to coordinate benefits, if a Participant has coverage through another carrier.

Other Possible Uses and Disclosures of PHI

1. Required by Law: The Plan may use or disclose PHI when required by law, provided the use or disclosure complies with and is limited to the relevant requirements of such law;
2. Public Health and Safety: The Plan may use or disclose PHI when permitted for purposes of public health activities, including disclosures to:
    a. A public health authority or other appropriate government authority authorized by law to receive reports of Child abuse or neglect;
    b. Report reactions to medications or problems with products or devices regulated by Federal Food and Drug Administration or other activities related to quality, safety, or effectiveness of FDA-regulated products or activities;
    c. Locate and notify persons of recalls of products they may be using; and
    d. A person who may have been exposed to a communicable Disease or may otherwise be at risk of contracting or spreading a Disease or condition, if authorized by law;
3. The Plan may disclose PHI to a government authority, except for reports of Child abuse or neglect, when required or authorized by law, or with the Participant's agreement, if the Plan reasonably believes them to be a victim of abuse, neglect, or domestic violence. In such case, the Plan will promptly inform the Participant that such a disclosure has been or will be made unless the Plan believes that informing them would place them at risk of serious harm (but only to someone in a position to help prevent the threat). Disclosure generally may be made to a minor's parents or other representatives although there may be circumstances under Federal or State law when the parents or other representatives may not be given access to the minor's PHI;
4. Health Oversight Activities: The Plan may disclose PHI to a health oversight agency for oversight activities authorized by law. This includes civil, administrative or criminal investigations; inspections; claim audits; licensure or disciplinary actions; and other activities necessary for appropriate oversight of a health care program, and compliance with certain laws;
5. Lawsuits and Disputes: The Plan may disclose PHI when required for judicial or administrative proceedings. For example, the Participant's PHI may be disclosed in response to a subpoena, discovery requests, or other required legal processes when the Plan is given satisfactory assurance that the requesting party has made a good faith attempt to advise the Participant of the request or to obtain an order protecting such information, and done in accordance with specified procedural safeguards;
6. Law Enforcement: The Plan may disclose PHI to a law enforcement official when required for law enforcement purposes concerning identifying or locating a suspect, fugitive, material witness or missing person. Under certain circumstances, the Plan may disclose the Participant's PHI in response to a law enforcement official's request if they are, or are suspected to be, a victim of a crime and if it believes in good faith that the PHI constitutes evidence of criminal conduct that occurred on the Sponsor's or Plan's premises;
7. Decedents: The Plan may disclose PHI to family members or others involved in decedent's care or payment for care, a coroner, funeral director or medical examiner for the purpose of identifying a deceased person, determining a cause of death or as necessary to carry out their duties as authorized by law. The decedent's health information ceases to be protected after the individual is deceased for 50 years;
8. Research: The Plan may use or disclose PHI for research, subject to certain limited conditions;
9. To Avert a Serious Threat to Health or Safety: The Plan my disclose PHI in accordance with applicable law and standards of ethical conduct, if the Plan, in good faith, believes the use or disclosure is necessary to prevent or lessen a threat to health or safety of a person or to the public;

10. Workers' Compensation: The Plan may disclose PHI when authorized by and to the extent necessary to comply with workers' compensation or other similar programs established by law and
11. Military and National Security: The Plan may disclose PHI to military authorities or armed forces personnel under certain circumstances. As authorized by law, the Plan may disclose PHI required for intelligence, counter-intelligence, and other national security activities to authorized Federal officials.

Required Disclosures of PHI

1. Disclosures to Participants: The Plan is required to disclose to a Participant most of the PHI in a Designated Record Set when the Participant requests access to this information. The Plan will disclose a Participant's PHI to an individual who has been assigned as their representative and who has qualified for such designation in accordance with the relevant State law. Before disclosure to an individual qualified as a personal representative, the Plan must be given written supporting documentation establishing the basis of the personal representation. The Plan may elect not to treat the person as the Participant's personal representative if it has a reasonable belief that the Participant has been, or may be, subjected to domestic violence, abuse, or neglect by such person, it is not in the Participant's best interest to treat the person as their personal representative, or treating such person as their personal representative could endanger the Participant; and
2. Disclosures to the Secretary of the U.S. Dept. of Health and Human Services: The Plan is required to disclose the Participant's PHI to the Secretary of the U.S. Department of Health and Human Resources when the Secretary is investigating or determining the Plan's compliance with the HIPAA Privacy Rule.

Instances When Required Authorization Is Needed From Participants Before Disclosing PHI

1. Most uses and disclosures of psychotherapy notes;
2. Uses and disclosures for marketing;
3. Sale of PHI; and
4. Other uses and disclosures not described in this section can only be made with authorization from the Participant. The Participant may revoke this authorization at any time.

Participant's Rights

The Participant has the following rights regarding PHI about him/her:

1. Request Restrictions: The Participant has the right to request additional restrictions on the use or disclosure of PHI for treatment, payment, or health care operations. The Participant may request that the Plan restrict disclosures to family members, relatives, friends or other persons identified by them who are involved in their care or payment for their care. The Plan is not required to agree to these requested restrictions;
2. Right to Receive Confidential Communication: The Participant has the right to request that they receive communications regarding PHI in a certain manner or at a certain location. The request must be made in writing and how the Participant would like to be contacted. The Plan will accommodate all reasonable requests;
3. Right to Receive Notice of Privacy Practices: The Participant is entitled to receive a paper copy of the plan's Notice of Privacy Practices at any time. To obtain a paper copy, contact the Privacy Compliance Coordinator;
4. Accounting of Disclosures: The Participant has the right to request an accounting of disclosures the Plan has made of their PHI. The request must be made in writing and does not apply to disclosures for treatment, payment, health care operations, and certain other purposes. The Participant is entitled to such an accounting for the six years priors to his/her request. Except as provided below, for each disclosure, the accounting will include: (a) the date of the disclosure, (b)

the name of the entity or person who received the PHI and, if known, the address of such entity or person; (c) a description of the PHI disclosed, (d) a statement of the purpose of the disclosure that reasonably informs the Participant of the basis of the disclosure, and certain other information. If the Participant wishes to make a request, please contact the Privacy Compliance Coordinator;

5. Access: The Participant has the right to request the opportunity to look at or get copies of PHI maintained by the Plan about them in certain records maintained by the Plan. If the Participant requests copies, they may be charged a fee to cover the costs of copying, mailing, and other supplies. If a Participant wants to inspect or copy PHI, or to have a copy of the individual's PHI transmitted directly to another designated person, they should contact the Privacy Compliance Coordinator. A request to transmit PHI directly to another designated person must be in writing, signed by the Participant and the recipient must be clearly identified. The Plan must respond to the Participant's request within 30 days (in some cases, the Plan can request a 30-day extension). In very limited circumstances, the Plan may deny the Participant's request. If the Plan denies the request, the Participant may be entitled to a review of that denial;
6. Amendment: The Participant has the right to request that the Plan change or amend their PHI. The Plan reserves the right to require this request be in writing. Submit the request to the Privacy Compliance Coordinator. The Plan may deny the Participant's request in certain cases, including if it is not in writing or if they do not provide a reason for the request; and
7. Fundraising contacts: The Participant has the right to opt out of fundraising contacts.

Questions or Complaints

If the Participant wants more information about the Plan's privacy practices, has questions or concerns, or believes that the Plan may have violated their privacy rights, please contact the Plan using the following information. The Participant may submit a written complaint to the U.S. Department of Health and Human Services or with the Plan. The Plan will provide the Participant with the address to file their complaint with the U.S. Department of Health and Human Services upon request.

The Plan will not retaliate against the Participant for filing a complaint with the Plan or the U.S. Department of Health and Human Services

Contact Information
Privacy Compliance Coordinator Contact Information:

Kathy Phelps
Director of Human Resources and Privacy Officer
Phone: 239-304-7074.

HIPAA SECURITY

Disclosure of Electronic Protected Health Information ("Electronic PHI") to the Plan Sponsor for Plan Administration Functions

STANDARDS FOR SECURITY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION ("SECURITY RULE")

The Health Insurance Portability and Accountability Act (HIPAA) and other applicable law shall override the following wherever there is a conflict, or a term or terms is/are not hereby defined.
The Security Rule imposes regulations for maintaining the integrity, confidentiality and availability of protected health information that it creates, receives, maintains, or maintains electronically that is kept in electronic format (ePHI) as required under HIPAA.

Definitions

- Electronic Protected Health Information (ePHI), as defined in section 160.103 of the Security Standards (45 C.F.R. 160.103), means individually identifiable health information transmitted or maintained in any electronic media.
- Security Incidents, as defined within section 164.304 of the Security Standards (45 C.F.R. 164.304), means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operation in an information system.

Plan Sponsor Obligations

To enable the Plan Sponsor to receive and use Electronic PHI for Plan Administration Functions (as defined in 45 CFR §164.504(a)), the Plan Sponsor agrees to:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of the Plan;
2. Ensure that adequate separation between the Plan and the Plan Sponsor, as required in 45 CFR § 164.504(f)(2)(iii), is supported by reasonable and appropriate Security Measures;
3. Ensure that any agent, including a subcontractor, to whom the Plan Sponsor provides Electronic

PHI created, received, maintained, or transmitted on behalf of the Plan, agrees to implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the Electronic PHI and report to the Plan any security incident of which it becomes aware; and

4. Report to the Plan any security incident of which it becomes aware.

Notification Requirements in the Event of a Breach of Unsecured PHI

The required breach notifications are triggered upon the discovery of a breach of unsecured PHI. A breach is discovered as of the first day the breach is known, or reasonably should have been known. When a breach of unsecured PHI is discovered, the Plan will:

1. Notify the Participant whose PHI has been, or is reasonably believed to have been, assessed, acquired, used, or disclosed as a result of the breach, in writing, without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. Breach Notification must be provided to individual by:
    a. Written notice by first-class mail to the Participant (or next of kin) at the last known address or, if specified by the Participant, e-mail;
    b. If the Plan has insufficient or out-of-date contact information for the Participant, the Participant must be notified by a "substitute form";
    c. If an urgent notice is required, the Plan may contact the Participant by telephone.

    The breach notification will have the following content:
    - Brief description of what happened, including date of breach and date discovered;
    - Types of unsecured PHI involved (e.g., name, Social Security number, date of birth, home address, account number);
    - Steps the Participant should take to protect from potential harm;
    - What the Plan is doing to investigate the breach, mitigate losses and protect against further breaches;

2. Notify the media if the breach affected more than 500 residents of a State or jurisdiction. Notice must be provided to prominent media outlets serving the State or jurisdiction without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered;
3. Notify the HHS Secretary if the breach involves 500 or more individuals, contemporaneously with the notice to the affected individual and in the manner specified by HHS. If the breach involves less than 500 individuals, an internal log or other documentation of such breaches must be maintained and annually submitted to HHS within 60 days after the end of each Calendar Year; and
4. When a Business Associate, which provides services for the Plan and comes in contact with PHI in connection with those services discovers a breach has occurred, that Business Associate will notify the Plan without unreasonable delay and in no case later than 60 calendar days after discovery of a breach so that the affected Participants may be notified. To the extent possible, the Business Associate should identify each individual whose unsecured PHI has been, or is reasonably believed to have been, breached.