HIPAA PRIVACY RULE AND SECURITY STANDARDS

This Plan complies with the requirements of § 164.504(f) of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, 45 C.F.R. parts 160 through 164 (the regulations are referred to herein as the "HIPAA Privacy Rule" and § 164.504(f) is referred to as "the "504" provisions") which establish the extent to which the Plan sponsor will receive, use and/or disclose Protected Health Information.

The Plan's Designation of Person/Entity to Act on its Behalf

The Plan has determined that it is a group health plan within the meaning of the HIPAA Privacy Rule, and the Plan designates Father Kevin Slattery to take all actions required to be taken by the Plan in connection with the HIPAA Privacy Rule (*e.g.,* entering into business associate contracts; accepting certification from the Plan sponsor).

The Plan's disclosure of Protected Health Information to the Plan sponsor – Required Certification of Compliance by Plan sponsor

Except as provided below with respect to the Plan's disclosure of summary health information, the Plan will (a) disclose Protected Health Information to the Plan sponsor or (b) provide for or permit the disclosure of Protected Health Information to the Plan sponsor by a health insurance issuer or HMO with respect to the Plan, only if the Plan has received a certification (signed on behalf of the Plan sponsor) that:

1. the Plan Documents have been amended to establish the permitted and required uses and disclosures of such information by the Plan sponsor, consistent with the "504" provisions;

2. the Plan Documents have been amended to incorporate the Plan provisions set forth in this section; and

3. the Plan sponsor agrees to comply with the Plan provisions as described by this section

Permitted disclosure of members' Protected Health Information to the Plan sponsor

The Plan (and any health insurance issuer or HMO servicing the Plan) will disclose members' Protected Health Information to the Plan sponsor only to permit the Plan sponsor to carry out plan administration functions. Such disclosure will be consistent with the provisions of this section.

All disclosures of the Protected Health Information of the Plan's members by a health insurance issuer or HMO to the Plan sponsor will comply with the restrictions and requirements set forth in this section and in the "504" provisions.

The Plan may not, and may not permit a health insurance issuer or HMO, to disclose members' Protected Health Information to the Plan sponsor for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan sponsor.

The Plan sponsor will not use or further disclose members' Protected Health Information other than as described in the Plan Documents and permitted by the "504" provisions.

The Plan sponsor will ensure that any agent(s), including a subcontractor, to whom it provides members' Protected Health Information received from the Plan (or from the Plan's health insurance issuer or HMO), agrees to the same restrictions and conditions that apply to the Plan sponsor with respect to such Protected Health Information.

The Plan sponsor will not use or disclose members' Protected Health Information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan sponsor.

The Plan sponsor will report to the Plan any use or disclosure of Protected Health Information that is inconsistent with the uses or disclosures provided for in the Plan Documents (as amended) and in the "504" provisions, of which the Plan sponsor becomes aware.

Notify *participants* of any *PHI* use or disclosure that is inconsistent with the uses or disclosures provided for of which the *Plan Sponsor*, or any *Business Associate* of the *Plan Sponsor* becomes aware, in accordance with the *health breach notification rule* (16 CFR Part 318); 1/1/17 63

Notify the Federal Trade Commission of any *PHI* use or disclosure that is inconsistent with the uses or disclosures provided for of which the *Plan Sponsor*, or any *Business Associate* of the *Plan Sponsor* becomes aware, in accordance with the *health breach notification rule* (16 CFR Part 318)

"Plan administration" activities are limited to activities that would meet the definition of payment or health care operations, but do not include functions to modify, amend or terminate the *Plan* or solicit bids from prospective issuers. *"Plan administration"* functions include quality assurance, claims processing, auditing, monitoring and management of carve-out plans, such as vision and dental. It does not include any employment-related functions or functions in connection with any other benefit or benefit plans.

Disclosure of members' Protected Health Information – Disclosure by the Plan sponsor

The Plan sponsor will make the Protected Health Information of the member who is the subject of the Protected Health Information available to such member in accordance with 45 C.F.R. § 164.524.

The Plan sponsor will make members' Protected Health Information available for amendment and incorporate any amendments to members' Protected Health Information in accordance with 45 C.F.R. § 164.526.

The Plan sponsor will make and maintain an accounting so that it can make available those disclosures of members' Protected Health Information that it must account for in accordance with 45 C.F.R. § 164.528.

The Plan sponsor will make its internal practices, books and records relating to the use and disclosure of members' Protected Health Information received from the Plan available to the U.S. Department of Health and Human Services for purposes of determining compliance by the Plan with the HIPAA Privacy Rule.

The Plan sponsor will obtain authorization prior to the sale of any Protected Health Information;
The Plan sponsor will, if feasible, return or destroy all members' Protected Health Information received from the Plan (or a health insurance issuer or HMO with respect to the Plan) that the Plan sponsor still maintains in any form after such information is no longer needed for the purpose for which the use or disclosure was made. Additionally, the Plan sponsor will not retain copies of such Protected Health Information after such information is no longer needed for the purpose for which the use or disclosure was made. If, however, such return or destruction is not feasible, the Plan sponsor will limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

The Plan sponsor will ensure that the required adequate separation, described below, is established and maintained.

Disclosures of Summary Health Information and Enrollment and Disenrollment Information to the Plan sponsor

The Plan, or a health insurance issuer or HMO with respect to the Plan, may disclose summary health information to the Plan sponsor, if the Plan sponsor requests the summary health information for the purpose of:

1. Obtaining premium bids from health plans for providing health insurance coverage under the Plan; or

2. Modifying, amending, or terminating the Plan.

The Plan, or a health insurance issuer or HMO with respect to the Plan, may disclose enrollment and disenrollment information to the Plan sponsor without the need to amend the Plan Documents as provided for in the "504" provisions.

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

The *Plan Sponsor* hereby authorizes and directs the *Plan*, through the *Plan Administrator* or the *third-party 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*.

Required separation between the Plan and the Plan sponsor

In accordance with the "504" provisions, this section describes the employees or classes of employees or workforce members under the control of the Plan sponsor who may be given access to members' Protected Health Information received from the Plan or from a health insurance issuer or HMO servicing the Plan.

(Classes may include, for example: Analyst/Administrators; Service Personnel; Information Technology Personnel; Clerical Personnel; Supervisors/Managers; Quality Assurance Unit)

1. Father Kevin Slattery
2. Bishop Joseph Kopacz
3. Benefits Coordinator
4. Chief Financial Officer

This list reflects the employees, classes of employees, or other workforce members of the Plan sponsor who receive members' Protected Health Information relating to payment under, health care operations of, or other matters pertaining to plan administration functions that the Plan sponsor provides for the Plan. These individuals will have access to members' Protected Health Information solely to perform these identified functions, and they will be subject to disciplinary action and/or sanctions (including termination of employment or affiliation with the Plan sponsor) for any use or disclosure of members' Protected Health Information in violation of, or noncompliance with, the provisions of this section.

The Plan sponsor will promptly report any such breach, violation, or noncompliance to the Plan and will cooperate with the Plan to correct the violation or noncompliance; to impose appropriate disciplinary action and/or sanctions, and to mitigate any deleterious effect of the violation or noncompliance.

Security Standards

Plan Sponsor Obligations

Where Electronic Protected Health Information will be created, received, maintained, or transmitted to or by the plan sponsor on behalf of the Plan, the Plan sponsor shall reasonably safeguard the Electronic Protected Health Information as follows:

A. Plan sponsor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that Plan sponsor creates received, maintains, or transmits on behalf of the Plan;

B. Plan sponsor shall ensure that the adequate separation that is required by 45 C.F.R. § 164.504(f)(2)(iii) of the HIPAA Privacy Rule is supported by reasonable and appropriate security measures;

C. Plan sponsor shall ensure that any agent, including a subcontractor, to whom it provides Electronic Protected Health Information agrees to implement reasonable and appropriate security measures to protect such Information; and

D. Plan sponsor shall report to the Plan any Security Incidents of which it becomes aware as descried below:

    1. Plan sponsor shall report to the plan within a reasonable time after Plan sponsor becomes aware, any Security Incident that results in unauthorized access, use, disclosure, modification, or destruction of the Plan's Electronic Protected Health Information; and
    2. Plan sponsor shall report to the Plan any other Security Incident on an aggregate basis every month, or more frequently upon the Plan's request.
    3. Notify *participants* of any *PHI* Security Incident of which the *Plan Sponsor*, or any *Business Associate* of the *Plan Sponsor* becomes aware, in accordance with the *health breach notification rule* (16 CFR Part 318);
    4. Notify the Federal Trade Commission of any *PHI* Security Incident of which the *Plan Sponsor*, or any *Business Associate* of the *Plan Sponsor* becomes aware, in accordance with the *health breach notification rule* (16 CFR Part 318).