MISSISSIPPI CONFERENCE OF THE UNITED METHODIST CHURCH BOARD OF MEDICAL BENEFITS
ORGANIZED HEALTH CARE ARRANGEMENT
AMENDED AND RESTATED HIPAA PRIVACY POLICIES AND PROCEDURES

1. **General:**

Mississippi Conference of the United Methodist Church Board of Medical Benefits (the **"Plan Sponsor"**) adopts these Amended and Restated HIPAA Policies and Procedures (the "**Privacy Policies and Procedures**"), effective August _____, 2016, in accordance with Title II of the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). These Policies and Procedures are hereby amended and restated in their entirety to comply with the requirements of HIPAA, the Health Information Technology for Economic and Clinical Health Act (**"HITECH Act"**), and their implementing regulations and guidance and are intended to be construed and interpreted in accordance with such laws.

The purpose of these Policies and Procedures is to establish guidelines to protect the confidentiality of protected health information (or **"PHI"**), which is defined as health information that:

(a) is created or received by a health care provider (a doctor or hospital), a health plan or Mississippi Conference of the United Methodist Church Board of Medical Benefits;

(b) relates to an individual's physical or mental condition;

(c) identifies an individual or can be used to identify an individual in conjunction with other information; and

(d) is in the possession and control of a covered entity (*i.e.* the self-insured group health plan sponsored by Mississippi Conference of the United Methodist Church).

Protected health information includes genetic information, which is defined broadly to include an individual's genetic tests, the genetic tests of family members (dependents and relatives up to the fourth degree), and the manifestation of a disease or disorder in family members. A genetic test is any analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes. Tests to evaluate cholesterol levels, blood count, liver function, or blood alcohol levels are not genetic tests.

The Plan Sponsor has designated certain health plans as an Organized Heath Care Arrangement (**"OHCA"**) on Exhibit A hereto. References to the OHCA in these Policies and Procedures shall include all health plans identified as members of such arrangement.

2. **Protections of Participants and Beneficiaries:**

The OHCA will not retaliate against or intimidate any participant or beneficiary who chooses to exercise his or her individual privacy rights, including the right to access protected

health information, the right to request amendment of protected health information, the right to an accounting of disclosures, the right to request certain privacy restrictions, and the right to receive notice of a breach of unsecured protected health information. The OHCA will not retaliate against or intimidate any person or organization that files a complaint with the Department of Health and Human Services about the OHCA's privacy practices, that participates in any investigation of the OHCA's privacy practices, or that opposes any act of the OHCA that may violate the privacy rules.

The OHCA will not require any participant or beneficiary to waive any right under the privacy rule, including the right to receive notice of a breach of unsecured protected health information, as a condition of enrollment in the OHCA or the receipt of benefits thereunder.

3. **Designation Of Privacy Official, Necessary Employees, and Business Associates:**

The Plan Sponsor shall designate a "**Privacy Official**" on Exhibit B hereto, who shall be responsible for the implementation and administration of these Policies and Procedures. The Privacy Official may delegate one or more of the duties hereunder to any Necessary Employee (as defined below) or other employee or officer of the Plan Sponsor. In carrying out his or her duties hereunder, the Privacy Official shall be entitled to engage such attorneys (who may include attorneys for the Plan Sponsor, whether employees or otherwise), consultants or other experts as he or she deems necessary or advisable.

The Plan Sponsor shall, from time to time, designate "**Necessary Employees**" on Exhibit B hereto, who shall be those employees and officers of the Plan Sponsor who are reasonably necessary to establish, maintain and administer the OHCA. Necessary Employees may be designated individually or by title or group. The Plan Sponsor shall designate the types of protected health information Necessary Employees reasonably require to carry out their duties relating to the OHCA.

The Plan Sponsor shall, from time to time, designate "**Business Associates**" on Exhibit B hereto, who shall be those persons providing services to or for the benefit of the OHCA and who have timely executed a Business Associate Agreement with the OHCA, such agreement in form and substance reasonably satisfactory to the OHCA, that satisfies the requirements for such agreements set forth in 45 C.F.R. 164.504(e) and the HITECH Act.

4. **Safeguarding PHI:**

Access to the records of the OHCA shall be limited to Necessary Employees and Business Associates, to the extent reasonably necessary to administer and maintain the OHCA. The OHCA and the Plan Sponsor shall safeguard all protected health information by using appropriate administrative, technical, and physical safeguards, as set forth below.

a. **Electronic records** containing PHI shall be accessed only by Necessary Employees. Electronic records containing enrollment and disenrollment information may be accessed by employees who are listed on Exhibit B hereto as Necessary Employees, provided such individuals (i) have been assigned a password, (ii) use such information to the minimum extent necessary, and (iii) receive training concerning the use and protection of such information.

b. **Paper records** related to the administration of the OHCA that contain PHI shall be maintained in accordance with the following safeguards:

i. Such records shall be stored under the direct supervision of one or more Necessary Employees.

ii. Such records shall be locked at all times. Only Necessary Employees shall access the records.

iii. Records containing protected health information that are to be destroyed must be stored in a locked facility pending destruction.

iv. Records containing PHI that are held in a document storage facility shall be identified and accessed only by Necessary Employees.

c. **Computer screens** and work stations used in connection with the operation or administration of the OHCA shall be subject to the following safeguards:

i. Necessary Employees shall ensure that protected health information is not readily visible from their workstations. All protected health information shall be placed in locked drawers when such employees must leave their workstations because of other duties or during non-work periods.

ii. Computer screens at workstations should not be visible to employees of the Plan Sponsor who are not designated as Necessary Employees.

d. **Oral communications** involving PHI shall be subject to the following safeguards:

i. Necessary Employees shall ensure the privacy of all conversations or discussions involving a participant or beneficiary or PHI.

ii. Conversations involving protected health information should take place only in enclosed offices or other private areas.

e. **Facsimile communications** involving PHI shall be made to/from Necessary Employees, shall be marked confidential or with a confidentiality message, and shall be sent/received to/at a location that is private or secure.

5. **Records and Record Retention:**

The Privacy Official (or its designee) shall cause to be maintained a written "Disclosure Log" for the purpose of recording any disclosure of PHI required under these Policies and Procedures. The Privacy Officer shall cause to be maintained such other logs or records as may be required by law. The following uses and disclosures of PHI shall be included in the Disclosure Log:

a. Disclosures of PHI required by law;

b. Disclosures of PHI for public health activities;

c. Disclosures of PHI for health oversight activities;

d. Disclosures of PHI concerning victims of abuse or neglect;

e. Disclosures of PHI pursuant to court order or subpoena; and

f. Such other disclosures of PHI as may require recordation in accordance with applicable law.

The Plan Sponsor shall retain (or cause to be retained) all records related to the implementation and operation of these Policies and Procedures for a period of six years, including, without limitation, the Disclosure Log or other log maintained by the Privacy Official, and any requests, notices or other communications required hereunder. Any additional records of the Privacy Official shall be maintained for a period of six years, measured from the date he or she ceased to serve. During such period, the records shall be deemed to contain PHI and shall be subject to the safeguards set forth herein.

6. **Required Disclosures of PHI:**

The PHI of an adult or emancipated minor shall be disclosed to him or her, except as to psychotherapy notes or information compiled in anticipation of or for use in a civil or criminal proceeding or administrative action. Such disclosures do not require an authorization and need not be recorded in the Disclosure Log. PHI shall be disclosed to the federal Department of Health and Human Services in connection with any audit of the OHCA's privacy practices.

7. **Permitted Uses and Disclosures of PHI:**

Except as otherwise provided below, the following uses and disclosures of PHI shall be permitted **without the consent or authorization of a participant or beneficiary**. Except as permitted by law, any disclosure of PHI shall be made to the minimum extent necessary and all disclosures shall be made in a manner intended to safeguard the privacy of participants and beneficiaries in the OHCA.

a. PHI can be disclosed to administer or facilitate the payment of claims or the determination of eligibility or coverage under the OHCA, including communication between a Necessary Employee and a Business Associate and communication between any Necessary Employee and the participant or beneficiary with respect to whom the claim relates. In addition, PHI can be disclosed to any person designated by the Privacy Official as engaged in the payment or administration of claims under the OHCA. These disclosures need not be recorded in the Disclosure Log.

b. PHI can be disclosed for health care operations, which shall include case management and care coordination, underwriting, premium rating, plan design or renewal, customer service, obtaining reinsurance, reviewing provider competence

or qualifications, claim audit and training. In addition, PHI can be disclosed to any person designated by the Privacy Official as engaged in health care operations. These disclosures need not be recorded in the Disclosure Log.

c. To any Business Associate. These disclosures need not be recorded in the Disclosure Log to the extent they relate to payment or health care operations.

d. PHI may be disclosed to the parent, guardian, or other personal representative of an unemancipated minor, subject to any limitations imposed under state law, except that such information shall not be disclosed if the Privacy Official reasonably believes that:

   i. The participant or beneficiary has been or may be abused or neglected by the personal representative; or

   ii. The participant or beneficiary will be endangered if the personal representative receives the information.

   These disclosures need not be recorded in the Disclosure Log.

e. For the treatment and payment activities of another covered entity.

f. Upon request by a health care provider, for that provider's treatment activities.

g. Upon request by another covered entity or a health care provider, to facilitate the requestor's payment activities, such as pursuant to a coordination of benefits provision.

h. Upon request by another covered entity, provided:

   i. The other entity has or had a relationship with the participant or beneficiary who is the subject of the PHI.

   ii. The health care operation is one of the following quality assessment and improvement, population-based activities relating to improving health or reducing health care costs, case management, conducting training programs, accreditation, certification, licensing, or credentialing, or health care fraud and abuse detection or compliance.

i. For judicial or administrative proceedings, subject to the following:

   i. All legal documents seeking PHI for judicial or administrative proceedings should be directed to the Privacy Official (or its designee), who will determine the appropriate response.

ii. PHI may be disclosed pursuant to a judicial order or judicial subpoena issued by a court or an administrative tribunal. The disclosure must be limited to the information expressly described in the order or subpoena; the Privacy Official shall not be required to ensure that the disclosure is limited to the minimum extent necessary.

iii. PHI may be disclosed pursuant to discovery requests and non-judicial subpoenas (not issued by a court or administrative tribunal), subject to the following:

1. The discovery request or subpoena is accompanied by a written statement showing that: (a) the requestor made a good faith attempt to provide written notice to the individual whose protected health information is requested, (b) the notice included enough information about the litigation such that the individual could raise an objection to the court/administrative tribunal, and (c) the time for the individual to raise objection has elapsed and no objections were filed or, if filed, have been resolved by the court.

2. The discovery request or subpoena is accompanied by a written statement showing that there is either a stipulated or court issued protective order that prohibits the use or disclosure of the protected health information outside the litigation, and requires that the protected health information be returned to the covered entity or destroyed at the conclusion of the proceeding.

3. If the discovery request or subpoena does not meet the requirements of either (1) or (2) above, the Privacy Official may disclose the requested protected health information by ensuring that the requirements in (1) and (2) above are satisfied.

iv. The Privacy Official shall designate a Necessary Employee who shall be responsible for the administration of this subparagraph i, including the receipt of all subpoenas and orders, communication with counsel, and the proper recordation of PHI released in accordance with the foregoing rules.

j. About a decedent; for this purpose, the OHCA shall treat any person authorized to act as the personal representative of a participant or beneficiary that is deceased as though he or she is the participant or beneficiary.

k. PHI may be disclosed for workers' compensation or similar purposes, in compliance with applicable state and federal laws. The Privacy Official shall designate an employee of the Plan Sponsor who shall (i) be familiar with any disclosures permitted or required under state and federal laws, (ii) shall record any such disclosure to the extent required by law, and (iii) shall receive training concerning the use and disclosure of PHI.

l. For health oversight activities, which shall consist of government benefit programs for which health information is relevant.

i. Health oversight agencies shall include the United States Department of Labor, the EEOC, the federal offices of inspectors general, the United States Department of Justice, OSHA, the Social Security Administration, the United States Food and Drug Agency, Medicaid fraud control units, state insurance departments and agencies and HHS Office for Civil Rights.

ii. Disclosures will be made if (1) the use or disclosure relates to a particular individual, and (2) the oversight activity is not directly related to the receipt of health care or qualification for public benefits related to health care.

m. Related to victims of abuse, neglect, or domestic violence, provided that the Privacy Official reasonably determines that a participant or beneficiary in the OHCA is the victim of abuse, neglect, or domestic violence, subject to the following:

i. Disclosure shall be made to a government authority authorized by law to receive reports of abuse, neglect, or domestic violence.

ii. The disclosure must be required by another law.

iii. The Privacy Official shall notify the participant or beneficiary of the disclosure, unless the official determines notification would harm the participant or beneficiary or if the appropriate disclosure would be to a personal representative, and it is the personal representative that is causing the abuse, neglect, or harm.

n. PHI can be disclosed for law enforcement purposes to a law enforcement official (i.e., someone having authority to investigate potential violations of law, or to prosecute or conduct criminal, civil, or administrative proceedings arising from alleged violations of the law), subject to the following:

i. Pursuant to a court order, warrant, subpoena, or summons issued by a judicial officer (including a grand jury subpoena).

ii. Pursuant to an investigative request from an administrative body, but only if the following additional conditions are met:

1. The Privacy Official determines that the information sought is relevant and material to a legitimate law enforcement inquiry;

2. The request is specific and limited in scope in light of the purpose for which the information is sought; and
3. De-identified information cannot reasonably be used.

iii. To identify or locate an individual, but only if officially requested. The PHI that may be disclosed in such circumstances shall be limited to name and address, social security number, type of injury, date and place of birth, ABO blood type and rh factor, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. (Note: information in the Plan Sponsor's regular employment or other records is not subject to the foregoing limitations.)

iv. About individuals who are suspected to be crime victims, but only if the individual agrees orally or in writing to the disclosure or the individual is unable to agree because of incapacity, in which case the Privacy Official may determine that disclosure is appropriate, but only if the following conditions are met:

1. The law enforcement official states that he or she needs the information to determine whether another person has violated the law; and

2. The law enforcement official states that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

o. About a crime relating to the OHCA.

p. To federal officials to avert a threat to national security or to conduct intelligence or other national security activities. These disclosures shall not be subject to recordation.

q. For research purposes; such information shall be de-identified to the extent practicable and the disclosure shall be subject to such consent, permission, disclosure or authorization requirements as may be imposed under applicable law.

8. **Restrictions on Uses and Disclosures of PHI:**

The OHCA shall not directly or indirectly receive remuneration in exchange for PHI of a participant or beneficiary unless, in accordance with 45 C.F.R. §164.508, the OHCA obtains a valid authorization from the participant or beneficiary whose PHI will be sold that includes a specification of whether the individual's PHI can be further exchanged for remuneration by the entity receiving PHI, except as otherwise allowed under the HITECH Act.

The OHCA shall not provide "marketing communications" to participants or beneficiaries or permit such communications to be provided unless the requirements set forth in 45 C.F.R. §164.501 as amended by the HITECH Act are satisfied.

The OHCA shall not use the genetic information of participants or beneficiaries for underwriting purposes, which includes determining whether a participant or beneficiary is eligible for benefits.

9. **Breach of Unsecured PHI:**

The OHCA will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, the Secretary of the Department of Health and Human Services ("Secretary"), and the media (when required) if the OHCA or one of its Business Associates discovers a breach of unsecured protected health information. The terms "breach" and "unsecured protected health information" shall have the meaning given in 45 CFR §164.402.

If the OHCA suspects or learns of an acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA, such occurrence shall be presumed to be a breach unless the OHCA or its Business Associate (if applicable) conducts a risk assessment and concludes that there is a low probability that the protected health information has been compromised. As part of the risk assessment, the OHCA shall evaluate the following factors:

a. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

b. the unauthorized person who used the PHI or to whom the disclosure was made;

c. whether the PHI was actually acquired or viewed;

d. the extent to which the risk to the PHI has been mitigated; and

e. whether the incident falls under one of the following exceptions, which does not require notice:

    i. unintentional access or use of PHI by a Necessary Employee or other employee of the Plan Sponsor;

    ii. inadvertent disclosure of PHI among Necessary Employees or representatives of another covered entity who are authorized to access PHI; or

    iii. unauthorized disclosure in which a person cannot access the information.

If the OHCA determines after its investigation that a breach has occurred, the OHCA will notify the **appropriate individual(s)** in accordance with the following rules:

a. Written notice of breach should be provided to the affected individual(s) without reasonable delay and in no event later than 60 calendar days after the OHCA discovers a breach.

b. Notice to the affected individual(s) shall include, to the extent possible, the following information:

i. a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

iii. any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. a brief description of what the OHCA is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

v. contact information for the OHCA, such as toll-free telephone number, an e-mail address, Web site, or postal address, for individuals to ask questions or learn additional information.

c. Notice to the affected individual(s) may be provided:

i. by first-class, United States mail to the individual's last known address; or

ii. by electronic mail, if the individual agrees to receive electronic notice and the agreement has not been withdrawn.

In any case deemed by the OHCA to require urgency because of possible imminent misuse of unsecured protected health information, the OHCA may provide information to the affected individual(s) by telephone or other means, as appropriate in addition to the notice provided in accordance with (i) or (ii) above.

d. Substitute notice must be provided if (i) the OHCA does not have sufficient contact information for some or all of the affected individuals; or (ii) some notices are returned to the OHCA as undeliverable. Substitute notice may be provided by an alternative form of written notice, telephone, posting, or other means allowed by law.

e. Notice may be provided to a parent or other personal representative if the affected individual is a minor or otherwise lacks legal capacity due to a physical or mental condition.

If a breach involves more than 500 residents of a State or jurisdiction, the OHCA shall provide notice to prominent media outlets (such as a newspaper, major television station, or major radio station) without reasonable delay and in no case later than 60 days after the discovery of

breach. This notice shall include the same information contained in the individual notice, which is set forth above.

The OHCA may delay providing notice in accordance with the above rules upon receipt of information from a law enforcement official that such notice would impede a criminal investigation or cause damage to national security. Such notice shall be delayed (a) for the time period specified in a written statement from the official or (b) 30 days from the date the OHCA receives an oral statement from the official. The OHCA shall retain a copy of any written statements from law enforcement officials and shall document all oral statements, including the name of the official, date, and substance of the statement.

In addition, the OHCA shall provide **notice of breach to the Secretary**. Such notice shall be provided in accordance with the following rules:

a. If the breach involves 500 or more individuals, the Secretary shall be notified immediately.

b. If the breach involves less than 500 individuals, the OHCA shall maintain a log or other information of such breach and submit it to the Secretary annually.

   i. Such log shall be provided to the Secretary not later than 60 days after the end of the calendar year in which such breach occurred.

   ii. The information shall be submitted to the Secretary in the manner specified on the HHS website.

The OHCA shall require its **Business Associates** to provide it with notice of a breach of unsecured protected health information so that the OHCA may comply with the notice requirements under law. The following rules apply to any notice provided by a Business Associate:

a. Written notice of breach should be provided to the OHCA without reasonable delay and in no event later than 60 calendar days after the Business Associate discovers a breach.

b. Notice shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the Business Associate, to have been accessed, acquired, used, or disclosed during the breach.

10. **Written Authorizations:**

The OHCA shall obtain written authorization for any use or disclosure of protected health information not described above or otherwise permitted under applicable law, subject to the following:

a. The OHCA shall not condition eligibility for enrollment or coverage upon the receipt of any authorization from a participant or beneficiary.

b. Unless the Privacy Official determines that an authorization is not required, written authorization shall be obtained for any use and disclosure not described above.

c. Any authorization shall be made, in writing, and shall specifically identify the PHI to be used or disclosed, to whom it will be disclosed, and the purpose of the disclosure.

d. Multiple authorizations may be combined for uses or disclosures of protected health information, except that an authorization may not be combined with any non-authorization document or with an authorization for the use or disclosure of psychotherapy notes.

Authorizations may be revoked at any time, by providing written notice to the Privacy Official. A revocation shall be effective upon its receipt by the Privacy Official, with respect to the disclosure of affected PHI made on or after its receipt.

Authorizations may be initiated by participants, beneficiaries, or other entities for the purpose of facilitating disclosure of protected health information to another entity. The Privacy Official shall review all such authorizations to ensure that the authorizations are complete. Disclosure shall not be made if an authorization is not sufficient. The OHCA's minimum necessary policy **does not** apply to uses or disclosures made pursuant to an authorization; disclosure shall be consistent with the terms of the authorization form.

11. **Disclosures To Family Members And Other Representatives:**

The OHCA will not disclose protected health information to a person who is involved in a participant's or beneficiary's health care or payment unless such participant or beneficiary has executed an Authorization to Share Health Information, except in the following limited circumstance:

a. If the inquiry is in person and the participant or beneficiary is present, and the OHCA obtains his or her verbal agreement that protected health information may be shared with the inquiring individual.

Any protected health information that is disclosed must be limited to that directly relevant to the inquiring individual's involvement in the participant's or beneficiary's health care and shall be to the minimum extent necessary.

Except as to an unemancipated minor, a participant or beneficiary shall be entitled to restrict such disclosure in accordance with Section 11 hereof. As to an unemancipated minor, he or she shall be entitled to restrict such disclosure to the extent expressly permitted by law.

These disclosures need not be recorded in the OHCA's Disclosure Log.

Note: This policy **does not** apply to inquiries by family members who are the personal representative of another family member. Personal representatives are generally treated as the

participant or beneficiary, and disclosures to these individuals need not be recorded in the Disclosure Log.

12. **Minimum Necessary:**

The OHCA, including Necessary Employees, shall use or disclose only the minimum necessary amount of protected health information to achieve the purpose of the use or disclosure. The phrase "minimum necessary" shall be interpreted in accordance with the HITECH Act. The Privacy Official may identify routine and recurring duties and obligations that require the use and disclosure of PHI in accordance with the provisions of these Policies and Procedures and determine the minimum necessary information required to comply with such routine duties. Otherwise, the Privacy Official shall review all non-routine uses and disclosures to determine the minimum necessary requirement.

The Privacy Official need not make a determination of minimum necessary when (a) disclosure is made to a public official pursuant to these Policies and Procedures, (b) disclosure is made to another covered entity, (c) when disclosure is made to a Business Associate for the purpose of carrying out the services under its agreement with the OHCA, or (d) when disclosure is made pursuant to an authorization.

13. **Rights of Participants and Beneficiaries:**

Subject to the limitations set forth herein, participants and beneficiaries of the OHCA shall be entitled to limit the use or disclosure of their PHI, request that communications to them about their PHI be conducted by alternative means or at alternative sites, access their PHI, amend or correct any inconsistencies or inaccuracies in their PHI, and request an accounting of the use of their PHI.

a. All requests shall be made, in writing, to the Privacy Official. The Privacy Official may develop standard forms and documents for this purpose, but shall not require the use of such forms. If a request is made in a nonstandard manner, it shall include sufficient information to permit the Privacy Official to administer the request, including the name address and telephone number of the participant or beneficiary, a description of the requested action, the identification of the person or persons with respect to whom any restriction is to apply, and such additional information as the Privacy Official deems necessary.

b. All requests and their disposition shall be recorded by the Privacy Officer in the OHCA's Disclosure Log.

c. As to any request to **restrict the use and disclosure of PHI**, the following additional rules shall apply:

    i. The Privacy Official shall respond to all completed requests promptly, but in no event later than 30 business days after receipt of a complete request, unless special circumstances require an extension of not more than 30 days.

ii. Subject to a limited exception that requires the Privacy Official to agree to restrict the disclosure of protected health information if a participant or beneficiary pays the health care provider out-of-pocket in full, the Privacy Official shall not agree to any limitation on the use and disclosure of PHI relating to the OHCA's payment of claims or health care operations. The Privacy Official shall reasonably accommodate all other requests, to the extent administratively feasible.

iii. The OHCA may terminate any restriction on the basis of administrative hardship, after disclosure to the affected participant or beneficiary.

iv. Any restriction on the use or disclosure of PHI or any revocation of a restriction made by the OHCA shall operate prospectively only.

d. As to any **request for confidential communications**, the affected participant or beneficiary shall specify why confidentiality is required, including an explanation of the circumstances under which disclosure of the information would endanger him or her. Any such request shall be granted to the extent administratively feasible.

e. As to any request for **access to PHI**, the following rules shall apply:

i. Any request shall apply only to PHI; documents that are not PHI and are not subject to access include an employee's personnel and separate medical file maintained by the Plan Sponsor as a business record in its capacity as an employer, performance evaluations, supervisors' notes, business records and the PHI of other participants and beneficiaries.

ii. A request for access shall be granted or denied within 30 days of the receipt for request, except that an additional 30 days shall be permitted if the PHI is stored off-site or if circumstances reasonably require.

iii. A request can be denied if (1) the information is not PHI, (2) the person requesting the information is an inappropriate personal representative, (3) the PHI includes psychotherapy notes, (4) the information was prepared or compiled in anticipation of litigation or administrative claim, (5) the information was obtained under a promise of confidentiality, or (6) access will endanger the life or physical safety of the participant or beneficiary or another person.

iv. If a request is denied for safety concerns, the participant or beneficiary can appeal the denial and the appeal shall be determined within 30 days by a Necessary Employee, other than the employee who made the initial determination.

f. As to any request for the **amendment of PHI or to supplement PHI**, the following rules shall apply:

i. A request shall be granted or denied within 60 days.

ii. A request may be denied if the Privacy Official determines the PHI is accurate and/or complete, the PHI was not created in the course of the operation and administration of the OHCA or the PHI is not subject to access (see above).

iii. The denial of a request is not subject to appeal, but a participant or beneficiary may submit a written statement of disagreement, which shall be appended to the disputed PHI and disclosed, with any subsequent disclosure of such PHI.

iv. If a request is granted, any correction or supplement shall be appended or linked to the PHI and furnished with any subsequent disclosure of such PHI.

g. As to any request for the **accounting of the disclosure** of PHI, the following rules shall apply:

i. The Privacy Official shall respond to any request not later than 60 days after receipt. If additional time is required, the participant or beneficiary shall be notified and an additional 30 days shall be available.

ii. A participant or beneficiary shall be entitled to an accounting once during each rolling 12-month period. If additional accountings are requested, the OHCA may assess its direct costs incurred in complying with the request.

iii. No accounting of records or disclosures for periods prior to April 14, 2004, shall be required. ***Drafting Note: Confirm HIPAA effective date—2004 or 2005.***

14. **Complaints:**

The Privacy Official shall receive and respond to all complaints about the administration of these Policies and Procedures. Upon receiving a complaint, the Privacy Official shall investigate and determine if there is any validity to the complaint. If the complaint is not valid, the Privacy Official shall notify the complaining individual, in writing. If the complaint is valid, the Privacy Official shall take such actions as may be reasonably necessary to correct any error or omission, including:

a. The amendment of these Policies and Procedures;

b. Notice or other sanctions imposed on any Business Associate involved in the error or omission;

c. The mitigation of any harm caused by the error and omission;

d. The imposition of sanctions against any Necessary Employee or other employee of the Plan Sponsor; or

e. The conduct of training intended to ensure that the error or omission does not recur.

15. **Mitigation of Harm:**

The OHCA shall mitigate, to the extent reasonably practicable, any harm caused by a use or disclosure of a participant's or beneficiary's PHI in violation of these Policies and Procedures. Upon learning of a violation of these Policies and Procedures, the Privacy Official shall determine whether a participant or beneficiary could be or has been harmed by the improper use or disclosure and whether there are any practicable steps that might have a mitigating effect with regard to such harm.

16. **Sanctions:**

The Privacy Official shall possess the authority to sanction any employee of the Plan Sponsor that uses or discloses a participant's or beneficiary's PHI or fails to notify the Privacy Official of a known or potential breach of unsecured protected health information in violation of these Policies and Procedures. Any use or disclosure of protected health information that potentially violates these Policies and Procedures should be reported directly to the Privacy Official. The Privacy Official shall investigate any alleged improper use or disclosure. Sanctions shall be imposed by the Privacy Official and shall be consistent with the Plan Sponsor's existing disciplinary policy.

MISSISSIPPI CONFERENCE OF THE UNITED METHODIST CHURCH BOARD OF MEDICAL BENEFITS
ORGANIZED HEALTH CARE ARRANGEMENT
HIPAA PRIVACY POLICIES AND PROCEDURES

EXHIBIT A
Organized Health Care Arrangement

The Mississippi Conference of the United Methodist Church Board of Medical Benefits health plans shall constitute an organized health care arrangement, consisting of the following component plans:

Benefit/Plan	Vendor/Insurer	Type of Arrangement
Medical Plan	Blue Cross Blue Shield (List states)	Self-insured
Dental Plan*	Delta Dental	Fully insured
Vision Plan*	EyeMed	Fully insured
Medical Expense Accounts	[To be inserted]	

*The dental and vision plans are listed as members of the OHCA for ease of administration. The dental plan is insured by Delta Dental, and the vision plan is insured by VSP. Participants and beneficiaries should refer to communications received from these respective insurance companies regarding privacy compliance for the dental and vision plans.

The following shall constitute joint compliance activities with respect to the health plans constituting the organized health care arrangement:

Function	Compliance
Participant Notice	All component plans
Policies and Procedures	All component plans
Necessary Employees and Privacy Official	All component plans
Training	All component plans
Plan Amendments	All component plans; Fully-insured or self-insured plans may adopt individual amendments that supercede joint compliance
Access Log	The company shall maintain different access logs with respect to its disclosures and uses; Business associates and fully-insured covered entities shall maintain separate logs

Function	Compliance
Physical Safeguards	The company shall establish appropriate physical safeguards as to PHI in its possession; Each business associate and fully-insured plan shall separately establish and administer physical safeguards
Records Retention	To the extent records are in the possession of the company, all records retention shall be jointly administered; Business associates shall establish a records retention policy satisfactory to the company; Fully insured plans shall separately adopt and administer records retention policies

MISSISSIPPI CONFERENCE OF THE UNITED METHODIST CHURCH BOARD OF MEDICAL BENEFITS
ORGANIZED HEALTH CARE ARRANGEMENT
HIPAA PRIVACY POLICIES AND PROCEDURES

EXHIBIT B
Designation of Privacy Official, Necessary Employees and Business Associates

1. **Privacy Official**: The Privacy Official shall be the Treasurer/Director of Finance & Administration/Conference Benefits Officer.

2. **Necessary Employees**: The Necessary Employees and their restrictions and limitations shall be:

Title/Function	**Usage / Limitations**
Treasurer/Director of Finance & Administrator/Conference Benefits Officer	Health plan operations; claims payment; settlor functions
Benefits Specialist	Health plan operations; claims payment; settlor functions
Human Resources Administrative Assistants	Health plan operations; claims payment
Human Resources Assistants	Health plan operations; claims payment
Controller	Minimum extent necessary
Treasurer	Minimum extent necessary
Payroll Administrators	Minimum extent necessary

3. **Business Associates:** The Business Associates of the OHCA shall be listed below. The OHCA shall enter into agreements with each such person in the time and manner required by law.

Name, Address, Contact Person	**Function**
Blue Cross Blue Shield	Third Party Administrator
Northwestern Mutual Life	Broker
LifeBux	Wellness Program Provider
Phelps Dunbar	Legal Advisor
[To be inserted]	Stop loss carrier
Horne, LLP	Auditor
[To be inserted]	Medical Expense Accounts

MISSISSIPPI CONFERENCE OF THE UNITED METHODIST CHURCH BOARD OF MEDICAL BENEFITS
ORGANIZED HEALTH CARE ARRANGEMENT
HIPAA PRIVACY POLICIES AND PROCEDURES

ACKNOWLEDGMENT

By execution below, I acknowledge that I have read the Mississippi Conference of the United Methodist Church Board of Medical Benefits Organized Health Care Arrangement HIPAA Privacy Policies and Procedures. I understand that effective as of [Insert Date] these Policies and Procedures have been amended and restated in their entirety, as a Necessary Employee I may have access to Protected Health Information, and I must comply with these HIPAA Privacy Policies and Procedures. I acknowledge that [To be inserted] is the Privacy Official and that I have been given the opportunity to ask questions about the HIPAA Privacy Policies and Procedures.

_____ _____

Signature Date

_____

Print Name

Retain the HIPAA Privacy Policies and Procedures and return this acknowledgement to the Privacy Official.