Southern Ohio Chamber Alliance Benefit Plan Trust

HIPAA Documentation Guide

Effective May 1st 2023

TABLE OF CONTENTS

1. USE AND DISCLOSURE PROCEDURES

INTRODUCTION

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") is a self-funded multiple employer welfare arrangement ("MEWA") providing medical benefits to the persons enrolled in and benefitting under the Arrangement ("Participants"). Employers ("Participating Employers") participate in the Arrangement by signing a participation agreement. The Arrangement is a non-plan MEWA within the meaning of Section 3(1) of the Employee Retirement Income Security Act of 1974, as amended ("ERISA") and each Participating Employer is a plan sponsor of its own single-employer plan (each is a "participating plan," and each of which is a part of the Arrangement). Individuals or entities may, as part of the Arrangement's administrative functions, have access to Participant's individually identifiable health information: (1) on behalf of the Arrangement itself, and/or (2) on behalf of entities ("subcontractors") performing necessary and essential Arrangement services.

The Health Insurance Portability and Accountability Act of 1996, as amended, ("HIPAA") is composed of two titles: Title I and Title II. Title I contains insurance reforms (related to access, portability, renewability) applicable to group health plans and individual policies. Title II contains provisions related to the prevention of fraud and abuse, and administrative simplification (including rules related to medical privacy and security). HIPAA's Title II requirements relating to privacy apply to group health plans generally, subject to some narrow exemptions which are not applicable to the Arrangement or any component plan. As such, HIPAA and the applicable regulations restrict the Arrangement's and each participating plan's ability to use and disclose protected health insurance ("PHI").

PHI means individually identifiable health information that is created or received by an entity covered by HIPAA (such as the Arrangement). PHI includes information that relates to any of the following: past, present or future physical or mental health or condition of a Participant; the provision of health care to a Participant; or the past, present or future payment for the provision of health care to a Participant.

"Individually identifiable" means health information that identifies the Participant or for which there is a reasonable basis to believe the information can be used to identify the Participant. PHI includes information of persons living or deceased.

For purposes of this Procedure, PHI does not include the following, referred to in this Procedure as "Exempt Information":

1. de-identified summary health information, as defined by HIPAA's privacy rules, that is disclosed to a Participating Employer solely for purposes of obtaining premium bids, or modifying, amending, or terminating its participation in the Arrangement (see below for a detailed discussion of de-identified "summary health information");

2. Arrangement enrollment and disenrollment information that does not include any substantial clinical information;

3. PHI disclosed to the Arrangement, the Southern Ohio Chamber Alliance Benefit Plan Trust, a participating plan, or a Participating Employer under a signed authorization that meets the requirements of the HIPAA privacy rules;

4. health information related to a person who has been deceased for more than 50 years;

5. information disclosed to the Southern Ohio Chamber Alliance Benefit Plan Trust or Participating Employer by an individual for functions that such entity performs in its role as an employer and not as sponsor of a group health plan or in providing administrative services to the Arrangement or a participating plan.

All individuals who have access to PHI must comply with these Use and Disclosure Procedures (the "Procedures"). Such individuals include associates, volunteers, trainees and other individuals who work under the direct control of the Arrangement or its subcontractors. The word "individual" as used in these Procedures includes all of these types of workers. An individual or entity that has access to PHI and who signs a Business Associate Agreement requiring the handling of PHI in accordance with these Procedures is a "Business Associate." "Business Associate" is defined in more detail below.

No third-party rights (including, but not limited to, the Participants, beneficiaries, dependents, heirs or Business Associates are intended to be created by these Procedures. The Arrangement reserves the right to amend the Procedures at any time (even retroactively) without notice.

A "Business Associate" for purposes of these Use and Disclosure Procedures is an entity or person that:

i. creates, receives, maintains, or transmits PHI on behalf of the Arrangement, and/or performs or assists in performing an Arrangement function or activity involving the use or disclosure of PHI (including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit and practice management, re-pricing, and the like); or

ii. provides legal, accounting, actuarial, consulting, data aggregation, brokerage, management, accreditation or financial services to or for the Arrangement where the performance of such services involves giving the service provider access to PHI.

PLAN RESPONSIBILITIES AS COVERED ENTITY

Appointment of Privacy Officer; Appointment of Contact Person for Questions

From time to time, the Arrangement's Board of Trustees will appoint a Privacy Officer and designate the Privacy Officer in a Trustee Resolution. Currently, Mark Hren of Consoliplex is the Privacy Officer. The Arrangement's Board of Trustees also will appoint someone to serve as the Contact Person for questions. Currently, the Plan Administrator is the Contact Person. The Board of Trustees may appoint the Privacy Officer to serve as the Contact Person. The duties of these two positions are described in greater detail below in the subsection entitled "Privacy Officer and Contact Person."

In sum, the Privacy Officer for the Arrangement will be responsible for developing and implementing the policies and procedures relating to HIPAA including, but not limited to these Procedures. The Contact Person will serve as the contact person for individuals that have

questions, concerns or complaints regarding the privacy rights under HIPAA. The Privacy Officer will coordinate the Arrangement's privacy activities with the Arrangement's Security Official.

Subcontractor Training

It is the Arrangement's policy to ensure that subcontractors train all new and current members of the subcontractor's workforce who have access to PHI. The Privacy Officer is responsible for ensuring subcontractors understand this training requirement so that individuals who have access to PHI receive the training necessary for them to carry out their duties under HIPAA. The Privacy Officer will ensure the subcontractors maintain their awareness of material changes in these Procedures.

Technical and Physical Safeguards

The Arrangement's Board of Trustees does not have access to PHI, however, from time to time may receive summary health information and de-identified health and financial data. A Participating Employer does not routinely have access to PHI, however, from time to time may receive summary health information and de-identified health and financial data. A Participating Employer may have access to PHI only to the extent the Participating Employer is permitted to receive PHI under the law and then, only if the Participating Employer has adopted all the policies, procedures, and plan amendments required under HIPAA, these Procedures, and by the terms of any agreement between the Participating Employer and the Arrangement's Board of Trustees. Detailed requirements are set forth in the below subsection entitled "Disclosures to Participating Employers." The Claims Administrator and certain other Business Associates have access to PHI.

The Arrangement has established appropriate technical and physical safeguards to prevent any intentional or unintentional use or disclosure of PHI that violate HIPAA. These safeguards also limit incidental uses and disclosures made pursuant to otherwise permitted or required uses and disclosures. Technical safeguards include limiting access to information by creating computer firewalls and requiring passwords that are changed periodically. Computers will be turned off when the user leaves the workstation for more than a few minutes and at the end of every day. Computer screens with PHI will be shielded from public view and the terminals will be located where access is limited. Any transmission of PHI by email will be done in a secure format.

Files containing PHI will be identified as such and will be stored in locked filing cabinets and/or locked rooms. Such files will be located where access is limited and will not be left unattended in the open. Any faxes containing PHI will be limited to fax machines that are located in secure areas.

These firewalls are designed to ensure that only authorized individuals will have access to PHI.

PRIVACY NOTICE

The Privacy Officer will either develop a notice explaining the Arrangement's privacy practices (the "Privacy Notice") or utilize the Department of Health and Human Services' model notice. The notice will list:

i. how the Arrangement can use and disclose PHI,

ii. an individual's rights under HIPAA, and

iii. the Arrangement's legal obligations with respect to PHI, and

iv. the Arrangement's complaint procedures, the name and address of the contact person for additional information and the date of the Notice.

The Privacy Notice will be distributed to everyone that has access to PHI under the Arrangement and additionally, will be provided to the Participants when the individual initially enrolls in the Arrangement, within sixty days of a material change to the notice, and anytime upon the individual's request. In addition, the Arrangement will notify Participants at least every three years that the Privacy Notice is available upon request.

Complaints

The Privacy Officer will be the Arrangement's contact person for receiving complaints. The Privacy Officer will create a log to record all complaints and will establish procedures for resolving complaints. A copy of the complaint procedures will be available to any Participant upon request (see Complaint Procedures, below).

Sanctions for Violations of Privacy Policy

The Arrangement does not have any employees. Sanctions for using or disclosing PHI in violation of HIPAA or this policy will be imposed in accordance with the Arrangement discipline policy for its Business Associates, up to and including termination of the contract.

Mitigation of Inadvertent Disclosures

The Arrangement shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of PHI in violation of HIPAA or this policy. If an individual or Business Associate becomes aware of an unauthorized use or disclosure, the individual or Business Associate must immediately contact the Privacy Officer so that appropriate steps can be taken to mitigate the harm.

No Intimidating or Retaliatory Acts

No individual or entity will intimidate, threaten, coerce, discriminate against or take any retaliatory action against any individual for exercising his or her rights, filing a complaint, participating in an investigation or opposing any improper practice under HIPAA.

Documentation

Because of the manner in which the Arrangement is established and operated, the Southern Ohio Chamber Alliance Benefit Plan Trust anticipates each Participating Employer will

have no access to PHI nor any access to electronic PHI ("ePHI"), however, if a Participating Employer should ever request to have access to any PHI or ePHI, the Participating Employer, prior to being given access to PHI, first must satisfy the requirements listed in the subsection below entitled "Disclosure to Participating Employer."

Procedures for Use and Disclosure

The Arrangement will use and disclose PHI only as permitted under HIPAA. For purposes of these Procedures "use" and "disclosure" will mean:

- **Use**. The sharing, employment, application, utilization, examination or analysis of PHI by any person working for or within the Arrangement or by a Business Associate.

- **Disclosure**. The release, transfer, provision of access to or divulging in any matter of PHI.

Entities That Must Comply with the Procedures

The following entities must comply with these Procedures:

1. Southern Ohio Chamber Alliance Benefit Plan Trust – Establishes the Arrangement. The Southern Ohio Chamber Alliance Benefit Plan Trust does not have access to PHI unless the Southern Ohio Chamber Alliance Benefit Plan Trust also is a Participating Employer and complies with the requirements applicable to Participating Employers (see plan amendment and other requirements outlined in the subsection entitled "Disclosure to Participating Employer," below).

2. Arrangement's Board of Trustees –The Trustees, acting in their capacity as Trustees, do not have access to PHI.

3. Claims Administrator – Anthem

4. Arrangement's Auditor – Maloney & Novotny

5. Arrangement Manager – Consoliplex Chambers, LLC

6. Producers. Producers do not have access to PHI.

7. Privacy Officer – Mark Hren

8. Other Service or Professional Providers

9. Participating Employers. Participating Employers only have access to PHI pursuant to a Participating Employer's specific request and then only to the extent the Participating Employer demonstrates compliance with the plan amendment provisions and other requirements outlined below under the subsection "Disclosure to Participating Employer."

Access to PHI is Limited to Business Associates

The entities listed above that have access to PHI may use and disclose PHI for the Arrangement administrative purposes. They may disclose PHI to other Business Associates that are permitted access to PHI for the Arrangement administrative functions. However, such disclosures will be limited to the minimum amount necessary to perform the Arrangement administrative function. Business Associates with access to PHI may not disclose PHI to Business Associates except those Business Associates that are permitted access to PHI and all disclosures will be in accordance with these Procedures. All Business Associates must enter into a Business Associate Agreement.

PERMITTED USES AND DISCLOSURES OF PHI

Uses for Payment and Health Care Operations

PHI may be used and disclosed for payment purposes and health care operations as permitted under HIPAA. For purposes of these Procedures "Payment" and "Health Care Operations" will mean:

A. **Payment**. Any activities taken to obtain the Arrangement contributions or to determine or fulfill the Arrangement's responsibility to provide benefits or to obtain or provide payment or reimbursement for the Arrangement benefits. Payment also includes:

i. Eligibility and coverage determinations including the coordination of benefits, adjudication and appeals of claims and benefit disputes, subrogation and reimbursement of the Arrangement claims as well as determining cost sharing amounts;

ii. Risk adjusting based on Participant status, case characteristics and demographics;

iii. Billing, claims management, any collection activities including premiums and reimbursements, obtaining payment under a contract for insurance or reinsurance (including stop loss coverage) and any related health care data processing; and

iv. Reviews for medical necessity or the appropriateness of care or justification of charges, utilization reviews including precertification, preauthorization, concurrent and retrospective reviews.

v. Any other payment activity that are permitted by the HIPAA privacy regulations.

B. **Health care operations.** The following activities are health care operations:

i. Conducting quality assessment and improvement activities;

ii. Reviewing plan performance and the competence, performance or qualifications of health care providers;

iii. Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract for health insurance or health

benefits as well as ceding, securing, placing or replacing any contract of reinsurance for risk related to claims under the Arrangement;

iv. Providing or arranging for medical review, legal services and auditing functions;

v. Business planning and development and disease management; and

vi. Business management and general administrative activities such as the implementation and compliance of these Procedures, resolution of internal grievances and other activities related to the Arrangement.

Uses by the Arrangement

A Business Associate may use and disclose a person's PHI for the Arrangement's own payment purposes or health care operations. Such disclosures will be limited to the "minimum necessary standards," as defined below. The disclosures will be documented in accordance with the documentation requirements listed below.

Disclosures for Another Entity's Payment Purposes

A Business Associate may disclose a person's PHI to another covered entity or health care provider so that the other covered entity or health care provider can conduct its payment activities. Such disclosures will be limited to the "minimum necessary standards," as defined below. The disclosures will be documented in accordance with the documentation requirements listed below.

Disclosures for the Operations of Health Care Operation

A Business Associate may disclose a person's PHI to another covered entity for that other entity's health care operations if the covered entity has or had a relationship with the person. Such disclosures must be approved by the Privacy Officer and will be limited to the "minimum necessary standards," as defined below. The disclosures will be documented in accordance with the documentation requirements listed below.

Disclosures and Use for Non-Health Benefits

Any Business Associate may use and disclose a person's PHI for other reasons only if:

1. the Business Associate obtains the person's authorization in accordance with the rules listed in these Procedures or an authorization is on file; and

2. the disclosure has been approved by the Privacy Officer.

Disclosures to Participating Employer

Participating Employers are entitled to receive PHI but only if the Participating Employer has certified, in writing, to the Privacy Officer that (1) the Participating Employer agrees to comply with the requirements of HIPAA including 45 C.F.R. § 164.504, and that the Participating Employer will provide adequate firewalls in compliance those rules, and additionally, to cause its participating plan to so comply, (2) has adopted the necessary policies and procedures required

under HIPAA, and (3) the Participating Employer has amended its participating plan document to provide the following and the Participating Employer will comply with those plan provisions:

- describe the employees or class of employees who may be given access to the PHI;
- restrict access to and use and disclosure by such individuals to plan administrative functions;
- ensure that there is adequate separation (also known as a firewall) between the participating employer's plan and the Participating Employer as sponsor of its own plan;
- ensure that any agents to whom it provides PHI agree to the same restrictions and conditions that apply to the Participating Employer;
- not use or disclose PHI for employment-related actions or for any other benefit or employee benefit plan of the Participating Employer;
- report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Participants, consider their requests for amendments to PHI, and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA privacy rules;
- make the Participating Employer's internal practices and records relating to the use and disclosure of PHI received from the Arrangement available to the Department of Health and Human Services ("HHS") upon request; and
- if feasible, return or destroy all PHI received from the Arrangement that the Participating Employer 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.
- Document and maintain the participating plan's privacy policies and procedures for at least six (6) years from the later of the date the policies were first created or first.

In such case, the Participating Employer may receive PHI but only with respect to individuals participating in the Arrangement by reason of that Participating Employer's participation in the Arrangement, and only to the extent necessary for the plan administrative functions to be performed by the Participating Employer.

Participating Employers may only receive ePHI if the above requirements are satisfied, and additionally, the Participating Employer's plan document must be amended to require the Participating Employer to: (1) implement administrative, physical, and technical safeguard that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that

the Participating Employer creates, receives, maintains, or transmits on behalf of its plan, (2) ensure that the firewall outlined above is supported by reasonable and appropriate security measure, (3) ensure that any agent or subcontractor to whom the Participating Employer provides ePHI agrees to implement reasonable and appropriate security measures to protect the ePHI, and (4) report any security incident of which the Participating Employer becomes aware.

Notwithstanding the foregoing, all Participating Employer may be able to receive:

De-Identified Information

As mentioned below, there are no restrictions on de-identified information. Therefore, the Arrangement may disclose de-identified information, as that term is defined by HIPAA, to the Participating Employer without restriction. The specific identifiers which must be removed to de-identify information are listed below.

Summary Health Information

The Arrangement also may disclose de-identified "summary health information" to the Participating Employer, as the plan sponsor, for insurance placement and to provide data to the Participating Employer so the employer can determine whether to modify, amend or terminate participation in the Arrangement as an employer or on behalf of a Participant.

Summary health information is information that summarizes the claims, history, expenses or types of claims by individuals for whom the Arrangement has provided health benefits under a group health plan. The information which must be removed from summary health information prior to disclosure is the same as the information that is removed to de-identify PHI generally, except that the geographic information described in (2) below need only be aggregated to the level of a five-digit zip code when providing summary health information.

A covered entity can disclose de-identified information provided the covered entity has no actual knowledge that the information could be used to identify the subject of the information (alone or in combination with other information); and removes the following 18 specific identifiers from the information. The 18 identifiers that must be removed to de-identify information are:

1. Names;

2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and their equivalent geocodes, except for the initial three digits of a ZIP code if, according to the current publicly available data from the Bureau of Census, (1) the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people, and (2) the initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;

3. all elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date and date of death and all ages over 89 and

all elements of dates (including year) indicative of such age except that such ages and elements may be combined into a single category of age 90 or older;

4. telephone numbers;

5. fax numbers;

6. email addresses;

7. Social Security Numbers;

8. medical record numbers;

9. health plan beneficiary numbers;

10. account numbers;

11. certificate or license numbers;

12. vehicle identifiers and serial numbers including license plates;

13. device identifiers and serial numbers;

14. web universal resource locators ("URLs");

15. internet protocol ("IP") address numbers;

16. biometric identifiers, including finger and voice prints;

17. full face photographic images and any comparable images; and

18. any other unique identifying number, characteristic or code.

Enrollment Information

The Arrangement may disclose to the Participating Employer who is enrolled and who has dis-enrolled in the Arrangement.

Pursuant to Authorization

Each Participating Employer previously has acknowledged and is aware that the Participating Employer has no right to PHI unless the Participating Employer has certified, in writing and demonstrated to the Privacy Officer that it will comply with HIPAA and satisfies the above listed requirements.

Individuals requesting access to their own PHI should direct their request and authorization to the Claims Administrator.

All disclosures under this section of the Procedures will be limited to the "minimum necessary standards," as defined below. The disclosures will be documented in accordance with the documentation requirements listed below.

All Business Associates are required enter Business Associate Agreements and are required to ask the Privacy Officer if they are unsure whether the task they are performing would allow the use or disclosure of any PHI.

Disclosures in Mandatory Circumstances

A Business Associate will disclose a person's PHI under the following circumstances:

Request from Individual. A Business Associate will disclose a person's PHI upon receiving a request from the individual or that individual's Authorized Representative (a Participant may authorize a personal representative, which may be an entity or an individual as their "Authorized Representative to receive PHI). Such disclosures will be made in accordance with the rules listed the section entitled "Disclosures to Individuals Under Right to Access Own PHI."

Request from Department of Health and Human Services. A Business Associate will comply with a request from the Department of Health and Human Services ("HHS") to disclose a person's PHI. The Business Associate will verify and document the disclosure in accordance with the terms listed below.

Disclosure required by Law. A Business Associate will comply with a request for disclosure if required by law.

Disclosures in Circumstances Permitted by Privacy Officer

A Business Associate who receives a request to disclose a person's PHI under the following circumstances will contact the Privacy Officer and the Privacy Officer will decide whether the PHI will be disclosed.

Request for Legal or Public Purpose. The following requests are requests for legal or public purposes:

i. Requests concerning victims of abuse, neglect or domestic violence - The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and the information will not be used against the individual and is necessary for an imminent enforcement activity. If this is the case, the individual must be promptly notified of the disclosure unless such notification would place the individual at risk or if informing the person would involve the personal representative who may be responsible for the abuse, neglect or violence.

ii. Judicial and administrative request - The disclosure: (1) is pursuant to a court or administrative tribunal order, or (2) is ordered under a subpoena, discovery request or other lawful process. Such disclosure may be made if the request is accompanied by assurances that the individual has been given notice of the request or the party seeking the information has made reasonable efforts to receive a qualified protective order.

iii. Request by or for law enforcement purposes - The disclosure is pursuant to a process and as otherwise required by law but only if the information requested is

specifically identified, relevant and material. The information must be limited to amounts reasonably necessary and cannot be de-identified. The information must be:

a. used to identify or locate a suspect, fugitive, material witness or missing person;

b. about a suspected victim of a crime if the person agrees to the disclosure or, if the person does not agree with the disclosure, the information will not be used against the person, and it is in the best interest of the person to disclose the information;

c. about a deceased individual and the person's death may have been a result of criminal activities; or

d. about suspected criminal activity that occurred on the Company's property.

iv. Disclosures to public health authorities for public health activities.

v. Disclosures to health oversight agency for health oversight activities.

vi. Disclosures to a coroner or medical examiner for purposes of identifying a deceased individual, determining the cause of death or any other reason authorized by law.

vii. Disclosures for organ donations for transplant activities.

viii. Disclosures for certain limited research activities.

ix. Disclosures based on a good faith belief that such disclosures will avert serious threats to health or safety.

x. Disclosures for specialized government functions, including of an inmate's PHI or disclosures to federal official for national security purposes.

xi. Disclosures to the extent necessary to comply with workers' compensation and other similar statutes.

All these types of disclosures must be approved by the Privacy Officer and must comply with the "minimum necessary standards," as defined below and documentation requirements listed below.

Disclosures Pursuant to Authorization

All requests to disclose a person's PHI to a third party (i.e., someone other than the person whose PHI is being disclosed) that is not required or permitted under these Procedures may be made pursuant to an authorization provide by the person whose PHI is the subject of disclosure. The following procedures apply to requests made pursuant to an authorization:

i. The identity of the individual (or the individual's representative) must be verified in accordance with the rules listed below;

ii. The authorization must be on a form approved by the Privacy Officer and the associate will verify that:

a. the form is properly signed and dated by the individual or the individual's representative,

b. the authorization has not expired or been revoked,

c. the request clearly describes the information to be used or disclosed,

d. clearly identifies the person or entity that is to receive the PHI,

e. the authorization includes a statement that the individual may revoke the authorization and includes the procedures to revoke the authorization, and

f. the authorization includes a statement about the possibility of subsequent re-disclosure of the information.

All uses and disclosures of PHI made pursuant to an authorization must be consistent with the terms and conditions listed on the authorization and all disclosures must be documented in accordance with the rules listed below.

Disclosures to Business Associates

All uses and disclosures of PHI to and by a Business Associate must be made in accordance with a valid Business Associate Agreement. All disclosures to Business Associates will be subject to the "minimum necessary standards," as defined below and documentation requirements listed below.

Disclosures to Family Members and Friends

The Arrangement will not disclose PHI to a person's family members and friends except as required or permitted by HIPAA. As a general proposition, authorization is required before a person's family or friends may have access to the person's PHI. The following rules apply whenever a Business Associate receives a request by a family member or friend to access a person's PHI:

i. If the request is by a friend or family member and the friend or family member is either:

a. the parent of the person and the person is a minor child, or

b. the friend of a family member is a representative of the person, then the Business Associate will comply with the verification procedures listed below.

ii. After the Business Associate has verified the family member as the person's parent or has verified the family member or friend is the person's representative, the Business Associate will comply with the rules applicable to Requests for Individual Access.

iii. All other requests by family members and friends to access a person's PHI must be made pursuant to the rules applicable to Disclosures Pursuant to Authorization.

Disclosures of De-Identified Information

There are no restrictions on the Arrangement's use and disclosure of de-identified information (defined above). The Privacy Officer must determine if the information is, in fact, de-identified information and must approve of the disclosure and/or use of the de-identified information.

The Privacy Officer must ascertain that the health information is de-identified either by professional statistical analysis or by removing the eighteen specific identifiers previously described in more detail above under the description of de-identified information.

Verification of Identity of Those Requesting PHI

The Privacy Officer must verify the identity of individuals requesting PHI. The Privacy Officer must also verify the authority of anyone having access to PHI if the Business Associate does not know the person's identity or authorization. The verification process varies depending on who is requesting the information.

Request by the Individual

When an individual requests access to his or her own PHI the Privacy Officer should:

i. Request a form of identification from the individual. A Business Associate may rely on a valid driver's license, passport or similar government issued photo identification.

ii. Verify the identification matches the identity of the individual requesting access to the PHI.

iii. Make a copy of the identification provided by the individual and include it in the individual's file.

iv. If an individual requests PHI over the telephone, the Business Associate must verify that individual's identity. The Business Associate should ask the person to identify his or her Social Security Number, birth date, address, their immediate supervisor and/or any other information the Business Associate needs to ascertain the identity of the individual.

v. All disclosures must be documented as listed below.

Request by Parent Seeking PHI of a Minor Child

Whenever a parent requests PHI for a minor child the Privacy Officer should:

i. First verify the person's identity and then request verification of the person's relationship with the child. This type of verification may be confirming the child's enrollment via the parent's enrollment in the Arrangement or some other method.

ii. Make a copy of the identification provided by the individual and include it in the individual's file.

iii. All disclosures must be documented as listed below.

Request by Personal Representative

Whenever a personal representative requests access to an individual's PHI the Privacy Officer should:

i. Request and make a copy of the documentation authorizing the person as the individual's personal representative.

ii. Verify the identification matches the identity of the individual requesting access to the PHI.

iii. Make a copy of all the documentation provided by the individual and include it in the individual's file.

iv. All disclosures must be documented as listed below.

Request by a Public Official

Whenever a request by a public official for an individual's PHI is made the Privacy Officer should:

i. If the request is made in person, the Business Associate must see the official's identification badge, or request a copy of any other official credentials verifying the person's government status.

ii. If the request is in writing, make sure the request is on appropriate government letterhead;

iii. If the request is by someone purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency such as a contract for services, memorandum of understanding or purchase order that establishes the person is acting on behalf of the public official.

iv. Request a written statement of legal authority under which the PHI is requested. If the request is made pursuant to a legal process, warrant, subpoena, order or other legal process the Business Associate should contact the Privacy Officer.

v. Obtain the Privacy Officer's prior approval for the disclosure.

vi. All disclosures must be documented as listed below.

Complying with the Minimum Necessary Disclosures

The Privacy Officer will ensure that, unless otherwise exempted, uses, disclosures and requests of PHI will be the minimum amount necessary to achieve the intended purpose of the use, disclosure or receipt.

PROCEDURES FOR DISCLOSURES.

There are two types of disclosure requests: recurring disclosure requests and non-recurring disclosure requests.

For recurring disclosure requests the Privacy Officer should identify the type of PHI to be disclosed and the person who is to receive the PHI. The Privacy Officer also should ascertain the conditions that apply to such access and the standards for disclosures to routinely hired Business Associates. After that, the Privacy Officer should identify the minimum amount of PHI that is necessary to accomplish the purpose of each of the recurring disclosure requests. Once the Privacy Officer has developed the policies and parameters of the recurring disclosure requests, the Business Associate should adhere those rules.

For all other requests (i.e., non-recurring disclosure requests) the Business Associate should contact the Privacy Officer so that the Privacy Officer can ensure the PHI disclosed in the minimum amount required to accomplish the purpose of the disclosure.

The rules governing the minimum necessary standards do not apply to the following uses and disclosures:

- Uses or disclosures to the individual;
- Uses or disclosures made pursuant to the individual's authorization;
- Disclosures made to the Department of Health and Human Services;
- Disclosures to or request by a health care provider for treatment;
- Uses or disclosures required by law; and
- Uses and disclosures required by HIPAA.

The Privacy Officer will refer to the Arrangement's Minimum Necessary Standard Procedure (outlined below) to determine if the use, disclosure or request of PHI complies with those Procedures.

Documentation

Business Associates will maintain copies of all the following information for at least six years from the later of the: (i) date the documents were created, or (ii) the date the documents were last effective:

- Notice of Privacy Practices.
- Whenever PHI is disclosed:

- the date of the disclosure;
- the name of the entity or person that received the PHI and, if available, the address of the person or entity;
- a brief description of the PHI disclosed;
- a brief description of the purpose the PHI was disclosed; and
- any other documentation required under these Procedures.

Mitigation of Unnecessary Disclosures

HIPAA requires that the Arrangement mitigate, to the extent possible, any damage resulting from any use or disclosure of PHI that violates these Procedures. Therefore, if any Business Associate becomes aware of any use or disclosure by the Arrangement, Business Associate or outside consultant or contractor, that violates these Procedures, the associate must immediately notify the Privacy Officer so the Privacy Officer can take steps to mitigate the damage to the individual.

COMPLAINT PROCEDURES

All complaints regarding the HIPAA privacy rules must be filed with the Privacy Officer on an approved form within ninety days of the alleged violation. The ninety-day period may be waived upon a showing of good cause for the delay in filing the complaint. The Privacy Officer will fully investigate the complaint and, if necessary, interview any relevant parties. The Privacy Officer will respond back to the person within thirty days of filing the complaint unless additional time is needed. If the Privacy Officer needs additional time the Privacy Officer will contact the person within thirty days of filing the complaint and tell the person additional time is needed and when the Privacy Officer anticipates responding to the complaint.

The person may appeal the Privacy Officer's finding by filing an appeal with the Southern Ohio Chamber Alliance Benefit Plan Trust's general counsel or their designee. The Southern Ohio Chamber Alliance Benefit Plan Trust's general counsel will fully investigate the complaint, review the Privacy Officer's findings and, if necessary, interview any relevant parties. The Southern Ohio Chamber Alliance Benefit Plan Trust's general counsel will respond back to the person within thirty days of filing the appeal unless additional time is needed. If the Southern Ohio Chamber Alliance Benefit Plan Trust's general counsel needs additional time, the Privacy Officer will contact the person within thirty days of filing the appeal and tell the person additional time is needed and when the General Counsel anticipates responding to the appeal.

If the person disagrees with the ruling from the Privacy Officer and the appeal to the Southern Ohio Chamber Alliance Benefit Plan Trust's general counsel, the person may file a complaint with the Secretary of the U.S. Department of Health and Human Services.

The person may file a complaint with the U.S. Department of Health and Human Services. The person can file the complaint over the internet at https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf.

Complaints may be filed in paper or email form with the Office of Civil Rights at the U.S. Department of Health and Human Services at the following email address: mailto:

OCRComplaint@hhs.gov. Alternatively, the person can file the complaint by mail or fax at the following address:

Centralized Case Management Operations
Department of Health and Human Services
Independence Avenue, S.W.
Room 509F HHH Bldg.
Washington, D.C. 20201

A person should check the HHS website for the most up to date information concerning the complaint process and timing: https://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html.

The Arrangement will not retaliate against anyone who files a complaint with the Privacy Officer and/or the Office of Civil Rights at the U.S. Department of Health and Human Services. In addition, the Arrangement and the Southern Ohio Chamber Alliance Benefit Plan Trust will never ask a person to waive his or her rights under HIPAA.

SANCTIONS FOR VIOLATION

A Business Associate that violates these Use and Disclosure Procedures will be subject to sanctions. Such sanctions may include, but are not limited to, oral and written warnings, suspension without pay and termination of employment. Unless the Privacy Officer determines otherwise, the sanctions will be as follows:

1. First Offense Oral Warning

2. Second Offense Written Warning

3. Third Offense Financial Penalty

4. Fourth Offense Termination of Agreement

All sanctions will be noted in the Business Associate's file. The Privacy Officer may waive a sanction.

PENALTIES FOR NON-COMPLIANCE

HIPAA imposes the following penalties for violating the privacy rules:

- Civil Penalties—$100 per incident up to $25,000 per person per year per standard; and

- Criminal Penalties—Up to:

  ➤ $50,000 and one year in prison for obtaining or disclosing PHI in violation of HIPAA;

  ➤ $100,000 and five years in prison for obtaining PHI under false pretenses; and

- $250,000 and ten years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

The amounts listed above may be indexed by the government. Although HIPAA does not create a personal cause of action under which a person can file a lawsuit, HIPAA does require the Arrangement Document to be amended to restrict the use and disclosure of PHI. Therefore, it is possible a person could file suit in Federal court against the Arrangement or a plan fiduciary claiming an ERISA violation.

2. SECURITY POLICY FOR EPHI

This Policy set forth the rules governing the use and disclosure of ePHI (defined above). It is the Arrangement's policy to fully comply with HIPAA and the Health Information Technology for Economic and Clinic Health Act ("HITECH") and all applicable rules and regulations as may be amended from time to time. For purposes of this Security Policy, PHI and ePHI do not include Exempt Information (defined in the Introduction section of the Use and Disclosure Procedures above).

Electronic Media means:

1. Electronic storage material on which data is or may be recorded electronically, including devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet, intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, voice via telephone, and facsimile, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

No third-party rights (including but not limited to the rights of Participants, beneficiaries, or covered dependents) are intended to be created by this Security Policy. The Arrangement reserves the right to amend or change this Security Policy at any time (and even retroactively) without notice. To the extent that this Security Policy establishes requirements and obligations above and beyond those required by HIPAA, the Security Policy shall be aspirational and shall not be binding upon the Arrangement or any person or entity. This Security Policy does not address requirements under state law or federal laws other than HIPAA.

1. Security Official

From time to time the Arrangement's Board of Trustees will name the Security Official for the Arrangement. Currently, Mark Hren is the Security Official for the Arrangement. The Security Official is responsible for the development and implementation of Arrangement policies and procedures relating to security, including but not limited to this Security Policy. To the extent the Security Official is a different person than the Privacy Officer, the Security Official will coordinate the Arrangement's security activities with the Privacy Officer. The appointment of the Security Official will be in writing and the Security Official will acknowledge, in writing, acceptance of that role.

2. Risk Analysis

From time to time, the Security Official will perform a risk analysis. The risk analysis consists of an eight-step process, including the following steps:

- ePHI boundary definition
- Threat identification
- Vulnerability identification
- Security control analysis
- Risk likelihood determination
- Impact analysis
- Risk determination
- Security control recommendations

The risk analysis will consider all relevant losses that would be expected if the security measures were not in place. 'Relevant losses' would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. The degree of response is determined by the risks identified. The risk assessment shall be periodically reassessed and updated as needed.

At the time this Security Policy is adopted, the Arrangement has no employees. All of the Arrangement's functions, including creation and maintenance of its records, are carried out by Business Associates of the Arrangement. Participating Employers have no access to PHI or ePHI and are not provided access to PHI or ePHI unless the Participating Employer satisfies the prerequisite requirements described above in the Use and Disclosure Procedures section of this document. The Board of Trustees do not receive PHI from the Arrangement.

The Arrangement does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Arrangement, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the third-party administrator, and other Business Associates. Accordingly, the Business Associates create, receive, maintain, and transmit all of the electronic PHI relating to the Arrangement, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Arrangement, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the Arrangement. The Arrangement has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Arrangement. That ability lies solely with the third-party administrator, and other Business Associates.

Because the Arrangement has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation, the third-party administrator, and other Business Associates affecting the security of the Arrangement's electronic PHI; and because the third-party administrator, and other Business Associates have undertaken certain obligations

relating to the security of electronic PHI that they handle in relation to the performance of administrative functions for the Arrangement, its policies and procedures, including this Policy, do not separately address the following Security Policy standards (including the implementation specifications associated with them):

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

The HIPAA security policies and procedures of the third-party administrator, and other Business Associates for electronic PHI of the Arrangement for the standards listed above are adopted by the Arrangement.

The Privacy Officer may assume all Business Associates (and their subagents) have the resources to conduct the risk analysis required under HIPAA and HITECH and that they have all conducted and are comply with the security requirements under HIPAA and HITECH.

3. Risk Management

The Arrangement relies on its third-party administrator and other Business Associates to manage risks to electronic PHI by limiting vulnerabilities, based on risk assessments, to a reasonable and appropriate level, taking into account the following:

- Their size, complexity, and capabilities;

- Their technical infrastructure, hardware, software, and security capabilities;

- The costs of security measures; and,

- The criticality of the electronic PHI potentially affected and the probability of the various risks.

Based on risk assessments undertaken by the third-party administrator, and the Arrangement's other Business Associates, the Arrangement made a reasoned, well-informed and good faith determination on the implementation of the HIPAA security regulations that it need not take any additional security measures, other than the measures set forth herein and the measures of the third-party administrator, and other Business Associates, to protect against reasonably anticipated threats and vulnerabilities and to reduce risks to the confidentiality, integrity and availability of electronic PHI.

4. Participating Employer's Plan Documents

Because of the structure of the Arrangement, Participating Employers do not have access to PHI or ePHI unless the Participating Employer specifically requests PHI or ePHI. If the Participating Employer requests PHI or ePHI, the Participating Employer must satisfy the requirements listed above under the section entitled "Disclosures to Participating Employer," including amendment to Participating Employer's participating plan document as described above.

5. Disclosures of Electronic PHI to Third-Party Administrator and Other Business Associates

- Business Associate is an entity (other than the Southern Ohio Chamber Alliance Benefit Plan Trust or a Participating Employer), such as a third-party administrator, that creates, receives, maintains, or transmits electronic PHI and:

- performs or assists in performing an Arrangement function or activity involving electronic PHI (including claims processing or administration, data analysis, underwriting, etc.); or

- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to the Arrangement's electronic PHI.

The Arrangement permits the third-party administrator and other Business Associates to create, receive, maintain, or transmit electronic PHI on its behalf. The Arrangement has obtained or will obtain satisfactory assurances from all Business Associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA security regulations and specifically providing that the Business Associate will:

- implement administrative, physical, and technical safeguards and documentation requirements that reasonably and appropriately protect the

confidentiality, integrity, and availability of the electronic PHI that the Business Associate creates, receives, maintains, or transmits on behalf of the Arrangement (the "Contract electronic PHI");

- ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of the Business Associate agree to comply with all of the requirements of the HIPAA security regulations to protect the Contract electronic PHI;

- report to the Arrangement any security incident or breach of unsecured PHI of which the Business Associate becomes aware;

- take any contractually required steps with respect to breach notification requirements; and

- authorize termination of the contract by the Arrangement if the Arrangement determines that the Business Associate has violated a material term of the contract.

6. Breach Notification Requirements

The Arrangement will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Arrangement or one of its Business Associates discovers a breach of unsecured PHI.

7. Documentation

The Arrangement's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of electronic PHI, and any necessary changes to policies or procedures will be documented and implemented promptly.

Except to the extent that they are carried out by Business Associates, the Security Official shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of any Participating Employer's plan document in accordance with this Security Policy, for example).

Policies, procedures, and other documentation controlled by the Arrangement may be maintained in either written or electronic form. The Arrangement will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The Arrangement will make its policies, procedures, and other documentation available to the Security Official and the Southern Ohio Chamber Alliance Benefit Plan Trust, the third-party administrator, and other Business Associates or other persons responsible for implementing the procedures to which the documentation pertains.

3. PRIVACY OFFICER and CONTACT PERSON

Privacy Officer.

HIPAA requires the Arrangement to designate a Privacy Officer to ensure the Southern Ohio Chamber Alliance Benefit Plan Trust and Arrangement comply with HIPAA. This document lists the Privacy Officer's responsibilities.

Position Title: Privacy Officer.

General Purpose: The Privacy Officer oversees all ongoing activities related to the development, implementation, maintenance of and compliance with the Arrangement's policies and procedures governing "protected health information" as that term is defined under HIPAA.

Responsibilities:

- Oversee the Southern Ohio Chamber Alliance Benefit Plan Trust's and Arrangement's overall compliance with the HIPAA privacy rule.

- Provides development guidance and assists in the identification, implementation, and maintenance of Arrangement information privacy policies and procedures in coordination with the Arrangement and internal and external parties.

- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the Arrangement's other compliance and operational assessment functions.

- Works with legal counsel, Arrangement's Manager, and the Arrangement's Board of Trustees to maintain appropriate privacy. confidentiality, consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

- Works with the Security Official (if this is a separate position) to ensure appropriate coordination between the privacy and security programs for the Arrangement.

- Oversees, directs, delivers, or ensures delivery of initial and ongoing privacy training and orientation to all associates, volunteers, subcontractors, alliances, Business Associates, and other appropriate third parties.

- Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and Business Associate Agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.

- Establishes with the Arrangement's Board of Trustees a process to track access to PHI, within the purview of the Arrangement and as required by law and to allow qualified individuals to review or receive a report on such activity.

- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's

workforce (if any), extended workforce (if any), and for all Business Associates, the information security official, administration, and legal counsel as applicable.

- Initiates, facilitates and promotes activities to foster information privacy awareness in the Arrangement and related entities.

- Reviews all system-related information security plans throughout the Arrangement.

- Works with all personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the Arrangement's policies and procedures and legal requirements to ensure the disclosure or use of the protected health information is appropriate.

- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.

- Serves as information privacy consultant to the Arrangement for all appropriate entities.

- Cooperates with the Department of Health and Human Services, the Office for Civil Rights, and any other appropriate government or legal entities in any compliance reviews or investigations.

Qualifications

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.

- Demonstrated organization, facilitation, communication, and presentation skills.

Contact Person.

HIPAA also requires group health plans to designate a Contact Person. The Privacy Officer and the Contact Person may be the same person, however, the responsibilities of the two positions are quite different. The responsibilities of the Contact Person are limited and nondiscretionary. In contrast, the responsibilities of the Privacy Officer require detailed knowledge and familiarity with HIPAA, the plans subject to HIPAA, Business Associates, and the Southern Ohio Chamber Alliance Benefit Plan Trust's and Participating Employer's involvement with administration of the Arrangement or participating group health plan. The Privacy Officer is more likely to be an ERISA fiduciary and to have access to sensitive PHI. Consequently, the Privacy Officer position generally requires a higher degree of sophistication and experience than the Contact Person position. These factors should be considered when designating individuals to serve in these positions.

Under HIPAA, the Contact Person is responsible for receiving privacy complaints and providing further information about matters covered by the Notice of Privacy Practices. The Contact Person has the following specific duties and responsibilities:

- Thoroughly documenting privacy complaints as they are received, including the name and contact information of the complainant and the nature of the complaint.

- If the Contact Person and Privacy Officer are different people, notifying the Privacy Officer of receipt of a complaint and providing any information regarding the complaint that is requested by the Privacy Officer.

- Ensuring that the Contact Person's name (or title) is correctly stated on the Notice of Privacy Practices.

- Thoroughly documenting inquiries regarding the Notice of Privacy Practices.

- Referring inquiries regarding the Notice of Privacy Practices to the Privacy Officer for response.

4. REPORTABLE BREACH NOTIFICATION POLICY

This Reportable Breach Notification Policy is adopted by the Arrangement as part of its HIPAA Privacy Policy and is intended to comply with the final HITECH regulations for breaches occurring on or after September 23, 2013 ("Breach Regulations"). Under the Breach Regulations, if a Reportable Breach of unsecured PHI has occurred, the Arrangement must comply with certain notice requirements with respect to the affected individuals, HHS, and, in certain instances, the media.

1. Identifying a Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If a Reportable Breach has not occurred, the notice requirements do not apply.

The Privacy Officer is responsible for reviewing the circumstances of possible breaches brought to his or her attention and determining whether a Reportable Breach has occurred in accordance with this Reportable Breach Notification Policy and the Breach Regulations. All Business Associates, and all workforce members (if any) who have access to PHI, are required to report to the Privacy Officer any incidents involving possible breaches.

Acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under HIPAA is presumed to be a Reportable Breach, unless the Privacy Officer determines that there is a low probability that the privacy or security of the PHI has been or will be compromised.

The Privacy Officer's determination of whether a Reportable Breach has occurred must include the following considerations:

- Was there a violation of HIPAA Privacy Rules? There must be an impermissible use or disclosure resulting from or in connection with a violation of the

HIPAA's privacy rules by the Arrangement or a Business Associate. If not, then the notice requirements do not apply.

- Was PHI involved? If not, then the notice requirements do not apply.

- Was the PHI secured? For electronic PHI to be "secured," it must have been encrypted to NIST (National Institute of Science and Technology) standards or destroyed. For paper PHI to be "secured," it must have been destroyed. If yes, then the notice requirements do not apply.

- Was there unauthorized access, use, acquisition, or disclosure of PHI? The violation of HIPAA's privacy rules must have involved one of these. If it did not, then the notice requirements do not apply.

- Does an exception apply? The Breach Regulations contain three narrow exceptions to breach notification (described below).

  ➤ Is there a low probability that privacy or security was compromised? If the Privacy Officer determines that there is only a low probability of compromise, then the notice requirements do not apply.

  ➤ If one of the following three exceptions applies, then a Reportable Breach has not occurred, and the notice requirements are not applicable.

    ▪ *Exception 1:* A Reportable Breach does not occur if the breach involved an unintentional access, use, or acquisition of PHI by a workforce member or Business Associate, if the unauthorized access, use, acquisition, or disclosure—(a) was in good faith; (b) was within the scope of authority of the workforce member or Business Associate; and (c) does not involve further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Arrangement were to mistakenly access the claim file of a Participant whose name is similar to the name of the intended Participant. However, the exception would not apply if an employee intentionally looked up a coworker's claim file out of curiosity.

    ▪ *Exception 2:* A Reportable Breach has not occurred if the breach involved an inadvertent disclosure from one person authorized by the Arrangement to have access to PHI to another person at the same covered entity or Business Associate also authorized to have access to the PHI, provided that there is no further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Arrangement inadvertently emailed PHI to the wrong coworker. However, if the same employee emailed the information to an unrelated third party, the exception likely does not apply.

- *Exception 3:* A Reportable Breach has not occurred if the breach involved a disclosure where the Arrangement has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI. For example, the exception may apply to an EOB mailed to the wrong person and returned to the third-party Claims Administrator unopened, or if a report containing PHI is handed to the wrong person, but is immediately retrieved before the person can read it. However, the exception does not apply if an EOB was mailed to the wrong person and the unintended recipient opened the envelope before realizing the mistake.

To determine whether there is only a low probability that the privacy or security of the PHI was compromised, the Privacy Officer must perform a risk assessment that considers at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, did the disclosure involve financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud? Did the disclosure involve clinical information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual? Did the use or disclosure otherwise further the unauthorized recipient's own interests?

- The unauthorized person who used the PHI or to whom the disclosure was made. For example, does the unauthorized recipient of the PHI have obligations to protect the privacy and security of the PHI, such as another entity subject to the HIPAA privacy and security rules or other privacy law? Would those obligations lower the probability that the recipient would use or further disclose the PHI inappropriately? Also, was the PHI impermissibly used within a covered entity or Business Associate, or was it disclosed outside a covered entity or Business Associate?

- Whether the PHI was actually acquired or viewed. If there was only an opportunity to actually view the information, but the Privacy Officer determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise. For example, if a laptop computer was lost or stolen and subsequently recovered, and the Privacy Officer is able to determine (based on a forensic examination of the computer) that none of the information was actually viewed, there may be no probability of compromise.

- The extent to which the risk to the PHI has been mitigated. For example, if the Arrangement can obtain satisfactory assurances (in the form of a confidentiality agreement or similar documentation) from the unauthorized recipient that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.

- If the Privacy Officer determines that there is only a low probability that the privacy or security of the information was compromised, then the Privacy Officer will document the determination in writing, keep the documentation on file, and not provide

notifications. On the other hand, if the Privacy Officer is not able to determine that there is only a low probability that the privacy or security of the information was compromised, the Arrangement will provide notifications.

2. If a Reportable Breach Has Occurred: Notice Timing and Responsibilities

If the Privacy Officer determines that a Reportable Breach has occurred, the Privacy Officer will determine (in accordance with the Breach Regulations) the date the breach was discovered in order to determine the time periods for giving notice of the Reportable Breach. The Arrangement has reasonable systems and procedures in place to discover the existence of possible breaches, and workforce members (if any) are trained to notify the Privacy Officer or other responsible person immediately so the Arrangement can act within the applicable time periods.

The Privacy Officer is responsible for the content of notices and for the timely delivery of notices in accordance with the Breach Regulations. However, the Privacy Officer may, on behalf of the Arrangement, engage a third party (including a Business Associate) to assist with preparation and delivery of any required notices.

The Breach Regulations may require a breach to be treated as discovered on a date that is earlier than the date the Arrangement had actual knowledge of the breach. The Privacy Officer will determine the date of discovery as the earlier of:

i. the date that a workforce member (other than a workforce member who committed the breach) knows of the events giving rise to the breach; and

ii. the date that a workforce member or agent of the Arrangement, such as a Business Associate (other than the person who committed the breach) would have known of the events giving rise to the breach by exercising reasonable diligence.

Except as otherwise specified in the notice sections that follow, notices must be given "without unreasonable delay" and in no event later than 60 calendar days after the discovery date of the breach. It is important to recognize that 60 days is an outside limit; in most cases, notification should be given much sooner. Accordingly, the investigation of a possible breach, to determine whether it is a Reportable Breach and the individuals who are affected, must be undertaken in a timely manner that does not compromise the notice deadline.

There is an exception to the timing requirements if a law-enforcement official asks the Arrangement to delay giving notices.

3. Business Associates

If a Business Associate commits or identifies a possible Reportable Breach, the Business Associate must give notice to the Privacy Officer. The Arrangement is responsible for providing any required notices of a Reportable Breach to individuals, HHS, and (if necessary) the media. The Arrangement may delegate responsibility for the notice requirement to a Business Associate, but only through a Business Associate contract.

Unless otherwise required under the Breach Regulations, the discovery date for purposes of the Arrangement's notice obligations is the date that the Arrangement receives notice from the Business Associate.

In its Business Associate contracts, the Arrangement will require Business Associates to:

- report incidents involving breaches or possible breaches to the Privacy Officer in a timely manner;

- provide to the Arrangement any and all information requested by the Arrangement regarding the breach or possible breach, including, but not limited to, the information required to be included in notices (as described below); and

- establish and maintain procedures and policies to comply with the Breach Regulations, including workforce training.

4. Notice to Individuals

Notice to the affected individual(s) is always required in the event of a Reportable Breach. Notice will be given without unreasonable delay and in no event later than 60 calendar days after the date of discovery (as determined above).

A. Content of Notice to Individuals

Notices to individuals will be written in plain language and contain all of the following, in accordance with the Breach Regulations:

- brief description of the incident.

- If known, the date of the Reportable Breach and the discovery date.

- A description of the types of unsecured PHI involved in the Reportable Breach (for example, full name, Social Security numbers, address, diagnosis, date of birth, account number, disability code, or other).

- The steps individuals should take to protect themselves (such as contacting credit card companies and credit monitoring services).

- A description of what the Arrangement is doing to investigate the Reportable Breach, such as filing a police report or reviewing security logs or tapes.

- A description of what the Arrangement is doing to mitigate harm to individuals.

- A description of what measures the Arrangement is taking to protect against further breaches (such as sanctions imposed on workforce members involved in the Reportable Breach, encryption, installation of new firewalls).

- Contact information for individuals to learn more about the Reportable Breach or ask other questions, which must include at least one of the following: Toll-free phone number, email address, website, or postal address.

B. Types of Notice to Individuals

The Arrangement will deliver individual notices using the following methods, depending on the circumstances of the breach and the Arrangement's contact information for affected individuals.

Actual Notice will be given in all cases, unless the Arrangement has insufficient or out-of-date addresses for the affected individuals. Actual written notice:

- will be sent via first-class mail to last known address of the individual(s);

- may be sent via email instead, if the individual has agreed to receive electronic notices;

- will be sent to the parent on behalf of a minor child; and

- will be sent to the next-of-kin or personal representative of a deceased person, if the Arrangement knows the individual is deceased and has the address of the next-of-kin or personal representative.

Substitute Notice will be given if the Arrangement has insufficient or out-of-date addresses for the affected individuals.

- If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, an alternate written notice, or other means.

- If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.

  ➤ Substitute notice via website. Conspicuous posting on home page of the website of the Arrangement or the Southern Ohio Chamber Alliance Benefit Plan Trust for 90 days, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. Contents of the notice can be provided directly on the website or via hyperlink.

  ➤ Substitute notice via media. Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. It may be necessary to give the substitute notice in both local media outlet(s) and statewide media outlet(s) and in more than one state.

- Substitute Notice is not required if the individual is deceased and the Arrangement has insufficient or out-of-date information that precludes written notice to the next-of-kin or personal representative of the individual.

Urgent Notice will be given, in addition to other required notice, in circumstances where imminent misuse of unsecured PHI may occur. Urgent notice must be given by telephone or other appropriate means. Example: Urgent notice is given to an individual by telephone. The Arrangement must also send an individual notice via first-class mail.

5. Notice to HHS

Notice of all Reportable Breaches will be given to HHS. The time and manner of the notice depends on the number of individuals affected. The Privacy Officer is responsible for both types of notice to HHS.

Immediate Notice to HHS. If the Reportable Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the date of discovery (as determined above). Notice will be given in the manner directed on the HHS website.

Annual Report to HHS. The Privacy Officer will maintain a log of Reportable Breaches that involve fewer than 500 affected individuals, and will report to HHS the Reportable Breaches that were discovered in the preceding calendar year. The reports are due within 60 days after the end of the calendar year. The reports will be submitted as directed on the HHS website.

6. Notice to Media (Press Release)

Notice to the media (generally in the form of a press release) will be given if a Reportable Breach affects more than 500 residents of any one state or jurisdiction. The Arrangement is not required to incur any costs to publish a media notice—the publication decision rests with the media outlet. Unlike notice to HHS, the residence of affected individuals is relevant for notice to the media.

If notice to the media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the date of discovery (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Officer is responsible for giving notice to the media.

5. MINIMUM NECESSARY STANDARD PROCEDURES

INTRODUCTION

One of the requirements under HIPAA is that, unless otherwise exempted, all uses, disclosures and requests of PHI be the minimum amount necessary to accomplish the intended purpose of the use, disclosure or receipt. It is the Privacy Officer's responsibility to ensure all use, disclosure and requests of PHI comply with this standard. Therefore, the Privacy Officer will apply the following procedures to determine if the use, disclosure or request of PHI complies with the HIPAA requirements limiting the amount of PHI used, disclosed or received.

DE-IDENTIFIED INFORMATION

There are no restrictions on the Arrangement's use, disclosure and receipt of de-identified information. Therefore, the Privacy Officer will first determine if the purpose of the intended use, disclosure or receipt of PHI can be accomplished by using de-identified information. If it can, then the Arrangement should use, disclose or request the de-identified information rather than use, disclose or request PHI.

De-identified information is health information that does not identify an individual with respect to which there is no reasonable basis to believe the information can be used to identify an individual and which has had removed the 18 identifiers described above.

The Privacy Officer must ascertain that the health information is de-identified either by professional statistical analysis or by removing the eighteen specific identifiers listed under HIPAA (and described above).

ACCESS TO PHI

If the Privacy Officer determines that the purpose of the intended use, disclosure or receipt of PHI cannot be accomplished by using de-identified information then the following procedures will apply to an associate's access to PHI. The following is a list of individuals that may have access to PHI and the type of PHI they may receive.

Participating Employer

Limited PHI Access. The Participating Employer will have access to PHI but only if the Participating Employer has adopted all the policies and procedures required under HIPAA and complied with the procedures described above under the subsection “Disclosures to Participating Employer.”

The Arrangement’s Board of Trustees

No PHI. The Arrangement’s Board of Trustees does not have access to PHI. The Claims Administrator handles claim adjudication and appeal processing and is the named fiduciary for those functions. The Board has access to various reports containing summary health information and de-identified health information.

Claims Administrator

Claims. Information regarding claims filed, claims re-pricing, claims paid, claims funding requirements, stop-loss submittals, stop-loss settlements, contributions, and checking accounts. The Claims Administrator handles claims adjudication and appeal processing and is the named fiduciary for those functions.

Medical Records. The Claims Administrator may request medical record information from the provider of service.

Appeals. Appeals, disputed claim/appeal necessary to properly evaluate the claim/appeal.

Enrollment. Applications for coverage, eligibility, enrollment, termination, disputed enrollment, COBRA coverage.

Arrangement Auditor

Claims. Information regarding claims filed, claims re-pricing, claims paid, claims funding requirements, stop-loss submittals, stop-loss settlements, contributions, and checking accounts.

Appeals. Appeals, disputed claim/appeal necessary to properly evaluate the claim/appeal.

Enrollment. Applications for coverage, eligibility, enrollment, termination, disputed enrollment, COBRA coverage.

Arrangement Manager

Claims. Information regarding claims filed, claims re-pricing, claims paid, claims funding requirements, stop-loss submittals, stop-loss settlements, Participant contributions, and checking accounts.

Enrollment. Applications for coverage, eligibility, enrollment, termination, disputed enrollment, COBRA coverage.

Claim Audit Report. De-identified claims data with some ability to determine PHI.

Arrangement Producer

No PHI. The Producer has health and financial information that needs to be kept secure. However, there is no PHI that the producer has as the information is received from the applicant and not from the Arrangement.

DISCLOSURE OF PHI

As described above, there are two types of disclosure requests. They are recurring disclosure requests and non-recurring disclosure requests. For recurring disclosure requests the Privacy Officer should identify the type of PHI to be disclosed and the person who is to receive the PHI. The Privacy Officer also should ascertain the conditions that apply to such access and the standards for disclosures to routinely hired Business Associates. After that, the Privacy Officer should identify the minimum amount of PHI that is necessary to accomplish the purpose of each of the recurring disclosure requests.

Recurring Disclosure Requests

The Privacy Officer has established the following rules for routine and recurring disclosures to implement and comply with the HIPAA requirements limiting the amount of PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure:

Claims Administrator.

To perform its duties relating to the Arrangement, the Claims Administrator will have access to PHI. The Claims Administrator is a fiduciary with respect to claims processing. For purposes of determining coverage, the Arrangement fiduciaries will have access to the person's claims file regarding the claim in question. For purposes of determining eligibility, the Claims Administrator will have access to all enrollment information of the Arrangement Participants and those individuals who have applied for coverage under the Arrangement. Claims Administrator of the Arrangement who review claims decisions and/or claims appeals requiring the use of discretion will have access to, and disclose, that amount of PHI as they may deem necessary, in the exercise of discretion and professional judgment, to render a claims determination or decide an appeal. For purposes of determining coordination of benefit issues, the Claims Administrator and other health plans or health insurance providers will have access to all enrollment information of the Arrangement's Participants who are the subject of the inquiry, as well as information regarding other coverage those Participants may have.

For underwriting purposes, the Claims Administrator will coordinate stop-loss carriers and managing general underwriters from whom quotes are obtained will have access to

aggregate claims information for the prior plan year, as well as such information regarding specific claims as are requested to determine the cause of unexpected claims that could influence the premium.

The Claims Administrator will have access to information regarding specific and aggregate claims as necessary to determine whether or not such claims are payable or reimbursable.

The Claims Administrator will have access to such medical records and medical information as they deem necessary to perform their duties related to pre-admission certification, concurrent review and retrospective review.

The Claims Administrator will be used by the Arrangement to provide COBRA administration services and will have access to such information relating to enrollment, eligibility, termination, COBRA elections and payment of COBRA premium as it deems necessary to perform its duties for the Arrangement.

The Claims Administrator will either contract with or by the preferred provider organizations providing discounts related to the Arrangement and will have access to all claims relating to services provided by member providers so that it may re-price such claims and resolve any disputes in connection the re-pricing.

The Claims Administrator will be the subrogation vendor used by the Arrangement and will have access to such medical records, accident information and claims information as it deems necessary to perform its duties relating to the Arrangement's subrogation interests.

Arrangement Auditor

The Arrangement Auditor will have information regarding claims filed, claims re-pricing, claims paid, stop-loss submittals, eligibility, enrollment, COBRA Participants, COBRA premiums, Participant contributions and checking accounts and to audit the Arrangement funds and assets.

Arrangement Manager

The Arrangement Manager will have access to all information needed to oversee and make decisions concerning the Arrangement operations, including claims costs, administrative costs, stop-loss premiums and provisions and audit reports.

Personal Representatives

A person's authorized representative will have access only to that portion of the person's PHI that relates to the purpose of their appointment if the authorized representative has been appointed for a limited purpose. (For example, if the authorized representative is appointed to only make decisions regarding the person's cancer treatment, the authorized representative will have access only to the person's PHI relating to cancer treatment.)

Attorneys

For purposes of providing legal services to the Arrangement, the Arrangement's attorneys will have access only to that class of PHI that relates to the issues on which the attorneys advise the Arrangement.

Producer

For purposes of providing advice to the Arrangement, the Producer will have no access to PHI. The Producer may have access to de-identified information as necessary to provide accurate and complete advice.

Printing and Mailing Services

Any printing and mailing service used by the Arrangement will have access to those documents to be printed and mailed, to perform its duties for the Arrangement.

Scanning and Scrubbing Services

Any scanning and/or claims “scrubbing” service(s) used by the Arrangement will have access to the documents to be scanned and the Arrangement's database required to perform the duties owed to the Arrangement.

Non-Recurring Disclosure Requests

The Privacy Officer will review each non-recurring request for PHI disclosure on an individual basis in accordance with the following rules. In addition, the Privacy Officer will consult with the party requesting the information to determine the purpose of the requested disclosure, if the purpose is not clear from the request. The Privacy Officer must understand the reason for the request and have sufficient expertise to understand and determine the minimum amount of PHI to be disclosed to achieve the intended purpose. If necessary, the Privacy Officer will consult with professionals to help determine the minimum necessary disclosure of PHI.

The Privacy Officer will consider the followings factors when limiting the amount of PHI to be disclosed by the Arrangement:

The requesting individual or entity must have a complete understanding of the purpose of the request for the PHI and explain, to the Privacy Officer's satisfaction, the purpose and that the information requested is no more than needed to meet the purpose; and all of the individuals or entities must be identified for whom the disclosure of PHI is required.

After considering the above, all requests for PHI should be directed to the Privacy Officer or the provider of health care service.

Special Circumstances

The Privacy Officer may, if reasonable under the circumstances, rely on a requested disclosure as the minimum necessary for the stated purpose(s) under special circumstances. The Privacy Officer will apply the following rules with respect to PHI disclosures under these special circumstances.

Public Officials

The Privacy Officer will approve disclosures to public officials if the disclosure is permitted under HIPAA.

Business Associate

The Privacy Officer will approve disclosures to a Business Associate if the Business Associate requests PHI to provide professional services to the Arrangement.

In all cases, the individual must provide documentation or represent that the PHI requested complies with the HIPAA requirements applicable to the minimum amount of disclosure necessary to comply with the intended purpose. The Privacy Officer is entitled to rely on the documentation or representation that the requested PHI requested complies with the HIPAA requirements applicable to the minimum amount of disclosure necessary to comply with the intended purpose.

REQUESTS FOR PHI

The Privacy Officer will ensure that all requests for PHI are limited to the minimum amount reasonably necessary to achieve the purpose for which the PHI was requested. The following procedures are established to limit the amount of PHI requested.

General Limits

Limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting PHI from the Arrangement;

Routine and Recurring Requests

For requests made on a routine and recurring basis, implement and comply with the policies and procedures that limit the PHI requested to the amount reasonably necessary to achieve the purpose of the request:

Arrangement Fiduciaries

Fiduciaries of the Arrangement who review claims decisions and/or claims appeals requiring the use of discretion will request only that amount of PHI as they may deem necessary, in the exercise of discretion and professional judgment, to render a claims determination or decide an appeal. The Board of Trustees will receive summary health information and de-identified information. The Claims Administrator is the named fiduciary for claims and appeals.

Eligibility Determinations

When the Claims Administrator is making eligibility determination, the Arrangement Administrator will request all enrollment information regarding those individuals who have applied for coverage under the Arrangement.

Coverage Determination

When coverage determinations are being made, the Claims Administrator will request the person's claims file regarding the claim in question.

Coordination of Benefits

When the Claims Administrator is determining coordination of benefit issues, the Claims Administrator and other health Arrangements or health insurance providers will request all enrollment information of the Arrangement Participants who are the subject of the inquiry, as well as information regarding other coverage those Participants may have.

Participating Employer

The Participating Employer is not entitled to receive PHI unless the Participating Employer certifies, in writing, to the Privacy Officer that it will comply with HIPAA and complies with the requirements listed above under the section “Disclosures to Participating Employer.” The Participating Employer will refer all requests to PHI to the Claims Administrator.

Arrangement Auditor

The Arrangement Auditor will request information regarding claims filed, claim re-pricing, claims paid, stop-loss submittals, eligibility, enrollment, termination, COBRA Participants, COBRA premiums, Participant contributions, checking accounts and to audit the handling of funds related to the Arrangement as well as the Arrangement assets.

Arrangement Manager

The Arrangement Manager will request all information regarding funding and expenses of the Arrangement, including but not limited to information regarding claims filed, claim re-pricing, claims funding requirements, claims paid, stop-loss submittals, COBRA premiums, Participant contributions and checking accounts from the Claims Administrator. The Arrangement Manager will request all information needed to oversee and make decisions concerning the Arrangement operations including claims costs, administrative costs, stop-loss premiums and provisions and audit reports. The Arrangement Manager will provide de-identified or summary health information to the Arrangement Board of Trustees for any decisions required by the Board.

For all other requests, the Privacy Officer will review each request on an individual basis in accordance with the rules listed below. In addition, the Privacy Officer may consult with the person requesting the information to determine the purpose of the requested disclosure, if the purpose is not clear from the request. The Privacy Officer will have an understanding of the Arrangement's privacy policies and procedures and sufficient expertise to understand and weigh the necessary factors. However, if necessary, the Privacy Officer will utilize the input of prudent professionals to assist in determining the minimum necessary request for PHI. The Privacy Officer will refer to the Claims Administrator any request for PHI.

The following rules will be used in limiting the amount of PHI provided:

1. The requesting individual or entity must have a complete understanding of the purpose of the request for the PHI and explain, to the Privacy Officer's satisfaction, the purpose and that the information requested is no more than needed to meet the purpose; and

2. All of the individuals or entities must be identified for whom the request for PHI is required.

3. After consideration of 1. and 2., the Privacy Officer will refer the requestor to either the Claims Administrator or the provider of health care service.

Requests for Entire Medical Record

If the request involves the individual's entire medical records, the request will be examined by the Privacy Officer, who will determine, in its discretion, whether the use, disclosure or request is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request. If necessary, the Privacy Officer will utilize the input of prudent professionals to assist in determining whether the use, disclosure or request is specifically justified.

The standard response for requests for entire or portions of medical record will be directed to the provider of health care services.

EXCEPTIONS TO THE MINIMUM NECESSARY STANDARDS

The rules governing the minimum necessary standards do not apply to the following uses and disclosures:

1. Uses or disclosures to the individual;

2. Uses or disclosures made pursuant to the individual's authorization;

3. Disclosures made to the Department of Health and Human Services;

4. Disclosures to or request by a health care provider for treatment

5. Uses or disclosures required by law; and

6. Uses and disclosures required by HIPAA.

The Privacy Officer may amend these rules at any time to comply with the HIPAA privacy rules.

6. DOCUMENT RETENTION PROCEDURES

One of the requirements under HIPAA is that the Arrangement allow an individual to request an accounting of certain disclosures of his or her PHI for up to the last six years. Also, the Arrangement must retain various documents to comply with HIPAA. To ensure that the Arrangement complies with the HIPAA reporting and retention requirements, the Arrangement hereby adopts the following document retention procedures.

Covered Documents

The following documents are subject to the document retention procedures:

1. To the extent it ever is provided to the Arrangement, a Participating Employer’s plan document and summary plan description booklet (“SPD”). Each Participating Employer has its own independent obligation under various laws to maintain a copy of its plan and SPD;

2. Any applicable benefit booklet;

3. All Arrangement policies and procedures implemented to comply with HIPAA;

4. All HIPAA Privacy Notices;

5. All signed HIPAA authorizations;

6. All requests by and responses to individuals with respect to (I) amending or correcting PHI (ii) accounting for PHI disclosures (iii) inspecting and copying PHI (iv) restricting the use and disclosure of PHI and (v) receiving confidential communications of PHI;

7. Records of PHI disclosures that are subject to the accounting rules under HIPAA;

8. All HIPAA complaints and the resolution of those complaints;

9. Copies of any HIPAA sanctions or investigations by the Secretary of the Department of Health and Human Services;

10. Copies of any sanctions against employees or Business Associates for violating the Arrangement's HIPAA procedures;

11. All Business Associate Agreements;

12. Summaries of all PHI that was destroyed by any Business Associate in accordance with a valid Business Associate Agreement;

13. Documentation from any Business Associate that certified it was not feasible to destroy PHI;

14. All training materials;

15. Copies of Participating Employer certifications required for the Participating Employer to have access to any PHI under this Policy.

Retention Period

All of the documents listed above shall be retained for a minimum of six years from the later of:

1. the date the document was created, or

2. the last day of the applicable Arrangement's year during which the document was last in effect.

Retention Format

The documents will be maintained in either electronic or hard copy format. If the documents are in electronic format that format will comply with all applicable statutes including HIPAA and ERISA.

Document Retention Procedure Amendment

The document retention procedures are adopted so that the Arrangement can comply with HIPAA reporting and retention requirements. The Board of Trustees retains the right to

amend the document retention procedures at any time with respect to current and future documents so that the Arrangement may comply with the HIPAA reporting requirements. In addition, the document retention Procedures will automatically be amended to comply with HIPAA as amended from time to time.

7. DOCUMENT PROVISIONS

As discussed above, the Board of Trustees do not have access to PHI. Also as discussed above, Participating Employers do not have access to PHI unless the Participating Employer has requested PHI and has satisfied all the requirements listed above under the subsection entitled “Disclosures to Participating Employers” including the required plan document provisions.

8. INSTRUCTIONS REGARDING NOTICE OF PRIVACY PRACTICES

HIPAA requires the Arrangement provide a notice of the Arrangement's privacy policy regarding PHI.

The notice explains how the Arrangement may use and disclose the person's PHI, the person's rights under HIPAA and the Arrangement's obligations regarding the PHI. This notice has to be provided to everyone who is covered under the Arrangement. In other words, if the Arrangement has or maintains a person's PHI, then the Arrangement has to provide that person the Arrangement's privacy notice. However, the Arrangement only has to provide the notice to the Participant in the Arrangement and not every family member. That is, the Arrangement will satisfy this notice obligation under HIPAA if it provides the privacy notice to just the Participant and does not have to provide the notice to each family member.

The Notice of Privacy Practices (“Notice”) has to be provided at the time an individual enrolls in the Arrangement. If the Arrangement's Notice is materially modified, everyone covered under the Arrangement must be provided the new Notice within sixty days of the change. In addition, the Arrangement is required to notify everyone once every three years that the Arrangement's Notice is available and tell people how to obtain a copy of the Notice.

HIPAA also states the privacy notice must be individually delivered to the person. However, no special or separate mailing is required. This means the notice can be included with a plan’s Summary Plan Description or in the enrollment materials. The notice can be delivered by e-mail if the person has agreed to electronic notice. Additionally, the person must have the right to request a paper copy of the notice.

The Arrangement should retain copies of the Notice for at least six years from the later of: (1) the date the notice was created, or (2) the notice's effective date.

9. SAMPLE FORMS AND NOTICES

Each form is designed to provide a template for the Privacy Officer or the Arrangement Manager to individualize based upon the specific requests by an individual participating in the Arrangement.

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT A – Sample Authorization for Release of Protected Health Information

I. Information about the use of Disclosure. This Authorization is required by the Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") to disclose my individually identifiable health information under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA").

I hereby authorize the Arrangement to use and disclose my individually identifiable protected health information as listed below. I understand this authorization is voluntary and I may revoke this authorization at any time by notifying the Arrangement, in writing, this authorization has been revoked.

Patient/Participant's Name: _____

Participant's Social Security Number: _____

Date of Birth: _____

Persons/organizations (or class of persons/organizations) authorized to use and disclose the information: _____

_____

_____

Persons/organizations (or class of persons/organizations) authorized to receive and use the information: _____

_____

_____

Specific description of information to be used and disclosed (including relevant dates(s) and conditions). The description should be specific enough so that the person receiving the authorization can clearly understand which information the authorization is intended to cover. For example, the description may include the dates when particular services were performed ("MRI performed in December 2018"). You may authorize disclosure of an entire medical record by writing "all health information": _____

_____

_____

Specific purpose of the disclosure. The statement "at the request of the individual" is sufficient when a participant/patient initiates the authorization and does not, or elects not to, provide a specific purpose:_____

_____

Will the health plan or health care provider requesting the authorization receive financial or in-kind compensation or remuneration in exchange for using or disclosing the health information described above?

No _____ Yes (describe) _____

This authorization will expire _____. The authorization must have an expiration date. This can be a specific calendar date or a specific time period (e.g., one year from the date the authorization is signed) or can be determined by reference to an event relating to the individual or to the purpose of the authorization (e.g., upon termination of enrollment in the health plan).

II. Important Information About Your Rights.

I understand that:

- This authorization is voluntary and I may refuse to sign it.
- I may revoke this authorization at any time prior to its expiration date by sending a written revocation notice to each entity that I previously authorized to disclose health information. The revocation will not have any effect on any actions that the entity took before it received the revocation notice.
- I am not required to sign this authorization as a condition to receiving treatment or payment for health care; enrolling in a health plan; or establishing eligibility for benefits.
- The information that is used or disclosed pursuant to this authorization may be redisclosed by the receiving person or organization and, upon redisclosure, may no longer be protected by federal privacy laws. *Note:* You have the right to seek assurances from the persons or organizations authorized to receive the information that they will not redisclose the information to any other party without your further authorization. You must request these additional assurances separately.

III. Signature of Patient/Participant or Patient's/Participant's Representative:

Signature of Patient/Participant or Person's Representative

_____	_____
Signature of Patient/Participant or Representative	Date
_____	_____
Printed Name of Patient/Participant Signing	Participant's Date of Birth

Relationship to Patient/Participant
Authorization Signing if Person is a
Representative

If the Person's Representative is signing this Authorization, the Representative must have a fully completed and signed Designation of Authorized Representative form.

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT B – Sample Designation of Authorized Representative

_____, do hereby appoint _____ as my authorized representative ("Authorized Representative") to act on my behalf for (check one):

_____ For all issues regarding my coverage under the Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement").

_____ For all issues relating to a specific claim (the "Claim") — Complete information below and attach pages describing the Claim with specificity.

My Authorized Representative shall have full authority to act and receive notices on my behalf with respect to either all of my information or, if I have indicated above that my Authorized Representative only represents me with respect to a specific claim, the initial determination of the Claim, any requests for documents relating to the Claim, and any appeal of an adverse determination of the Claim.

I understand that in the absence of a contrary direction from me, the Arrangement will, direct all information and notices to which I otherwise am entitled regarding all my benefits or just the Claim including benefit determinations, to my Authorized Representative only.

I am aware that the Standards for Privacy of Individually Identifiable Health Information set forth by the U.S. Department of Health and Human Services (the "Privacy Standards"), govern access to medical information. I understand that in connection with the performance of his/her duties hereunder, my Authorized Representative may receive my Protected Health Information, as defined in the Privacy Standards. I hereby consent to any disclosure of my Protected Health Information to my Authorized Representative.

This Designation of Authorization of Representative will expire (check one):

_____ This Designation of Authorized Representative will expire on _____ (insert specific date).

_____ This Designation of Authorized Representative will expire when the Claim listed on the attached page is finally adjudicated.

_____ This Designation of Authorized Representative will expire when I contact the Arrangement, in writing, stating that this Authorization has expired.

I have read this Designation of Authorized Representative and I understand the terms and I am signing this of my own free will. I hereby release the Arrangement from any liability for releasing any information pursuant to this Designation of Authorized Representative.

_____ _____

Signature of Person Date

ACKNOWLEDGMENT BY AUTHORIZED REPRESENTATIVE

I _____ have read the above Designation of Authorized Representative and I hereby accept this designation and agree to act as Authorized Representative for the person listed above.

_____ _____

Signature of Authorized Representative Date

Information to be sent to the Authorized Representative will be sent to the following address:

_____

Name

_____

Street Address

_____

City, State and Zip Code

If this Designation of Authorized Representative only pertains to a particular claim, please identify the claim by listing enough detail so that it can be identified. Examples may include the date and description of the type of injury or illness that resulted in the claim, the provider, etc.

_____

_____

_____

_____

_____

_____

_____

_____

Please return completed form to:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT C – Sample Request for Accounting of Protected Health Information

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") is subject to the privacy rules under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA").

HIPAA provides that a person enrolled in the Arrangement ("Participant") may request an accounting of certain disclosures of his or her protected health information ("PHI"). PHI means information that is created or received by the Arrangement and relates to the past, present or future physical or mental health or condition of a Participant; the provision of health care to a Participant; or the past, present or future payment for the provision of health care to a Participant; and that identifies the Participant or for which there is a reasonable basis to believe the information can be used to identify the Participant. PHI includes information of persons living or deceased.

A Participant may request an accounting of certain disclosures of PHI by the Arrangement. The Participant may use this form to request such an accounting.

I. Request for Accounting of Protected Health Information.

I request an accounting of disclosures of protected health information ("PHI") about me maintained in a "designated record set" held by the Southern Ohio Chamber Alliance Benefit Plan (the "Plan") in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its regulations. Please provide an accounting of disclosures of PHI that occurred during the following period (which cannot include any period more than six years before the date of this request):

_____

_____

I also understand that HIPAA provides the Arrangement does not have to account for certain disclosures of my PHI. Specifically, the Arrangement does not have to account for any disclosures made: (1) to carry out treatment, payment or health care operations; (2) to me about my own PHI; (3) pursuant to an authorization; (4) to any person involved with my care; (5) for specific national security or intelligence purposes; (6) to correctional institutions or law enforcement agencies; (7) as part of a "limited data set" as defined in HIPAA, which generally relates to research and public health purposes; (8) to assist in disaster relief; and (9) incidental to other permitted uses and disclosures of my PHI.

Except as otherwise provided below, for each disclosure, the accounting will include:

- the date of the disclosure;
- the name of the entity or person who received the PHI and, if known, the address of such entity or person;
- a brief description of the PHI disclosed; and

- a brief statement of the purpose of the disclosure that reasonably informs me of the basis for the disclosure. (If the disclosure was made in response to a request from another person or entity, the Arrangement may provide a copy of the request instead of a statement.)

II. Other Important Information

If, during the period covered by the accounting the Arrangement has made multiple disclosures of PHI to the same person or entity for a single purpose, then the accounting may provide the above-referenced information for the first disclosure, with the frequency or number of disclosures made during the accounting period, and the date of the last disclosure.

If, during the period covered by the accounting, the Arrangement makes its records available over a discrete period of time, then the accounting may include the range of dates (e.g., access was provided from August 1 to August 2, 2019; or during the week of August 12, 2019). Alternatively, if the disclosure is routinely made within a set period of time from an event, then the accounting may provide the date of the event and the normal interval.

If, during the period covered by the accounting the Arrangement has made disclosures of PHI for a particular research purpose for 50 or more individuals, then the accounting may provide certain information as permitted by HIPAA. If the Arrangement provides an accounting for research disclosures, and if it is reasonably likely that my PHI was disclosed for the research activity, then the Arrangement shall, at my request, assist in contacting the entity that sponsored the research and the researcher.

I understand that the Arrangement has 60 days to respond to this request. If the Arrangement is unable to provide a response within 60 days, then the Arrangement may extend the time for response by up to 30 additional days, so long as the Arrangement gives me a written statement of the reasons for the delay and the date by which the Arrangement will complete its action on the request. If this request is for a second or subsequent accounting within a 12-month period, then I agree to pay a reasonable, cost-based fee for the accounting.

III. Signature of Individual or Individual's Personal Representative

I ask that the accounting be mailed to me at:

_____
Name

_____
Street Address

_____
City, State and Zip Code

I agree to pay any fees for copying, etc. or I may withdraw this request if I have requested another accounting of my PHI within the last twelve months.

_____	_____
Signature of Patient/Participant or Representative	Date

Printed Name of Person Signing

Participant's Date of Birth

Relationship to Patient/Participant if Person Signing is an Authorized Representative

If the Person's Representative is signing, the Representative must include a fully completed and signed Designation of Authorized Representative Form.

This request must be completed and submitted to the Privacy Officer at the following address:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT D – Sample Response to Request for Accounting of Protected Health Information

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") is subject to the privacy rules under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA").

HIPAA provides that a person may request an accounting of certain disclosures of his or her protected health information ("PHI"). You have filed a request for such an accounting and this is the Arrangement's response to that request. The date of this response is _____.

I. Grant of Request

_____ Your request for an accounting of disclosures by the Arrangement of your PHI has been granted. The accounting is attached.

II. Grant of Request; Agreement to Pay Fees

_____ Your request for an accounting of disclosures by the Arrangement of your PHI has been granted. Because this request is for a second or subsequent accounting within a twelve-month period, you must agree to pay any fees for the accounting or withdraw or modify your request to avoid or reduce the fees. If you want to pay for the accounting, please indicate that below and return it to the Privacy Officer at the address listed below.

_____ I agree to pay the following fees for the accounting, which are reasonable and cost-based: $ _____

OR

_____ I hereby withdraw my request for an accounting.

OR

_____I hereby modify my request as follows: _____

_____

Please notify me if the fees will be avoided or reduced by modifying my request as indicated above.

_____ _____

Name of person receiving accounting Date

III. Need for Extension of Time

_____ The Arrangement received your request for an accounting of the disclosures of your PHI by the Arrangement on _____. The Arrangement is unable to provide your accounting within sixty days of the request for the following reason: _____

_____

The Arrangement will provide you the accounting within thirty days of this notice. If you have any questions, please contact the Arrangement's Privacy Officer:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

IV. No Disclosure Made

_____ No disclosures subject to the requirement to provide an accounting of disclosures have been made during the relevant time period.

V. Signature of Plan Representative

Name:_____

Signature:_____

Title:_____

Date:_____

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT E – Sample Request to Inspect or Copy Protected Health Information

I. Request to Inspect or Copy Protected Health Information

I request a copy of, or access to, protected health information ("PHI") in a "designated record set" (defined below) held by the Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA).

> A "designated record set" is a group of records maintained by or for the Arrangement including enrollment, payment, claims adjudication, and health plan case or medical management record systems; or records used by or for the Arrangement to make decisions about individuals. The term "record" means any item, collection, or grouping of information that includes PHI that is maintained, collected, used, or disseminated by or for the Arrangement.

I understand that I have the right to request an electronic copy of PHI in a designated record set, and the Arrangement must provide electronic PHI in the requested form and format if it is readily producible by the Arrangement. If the Arrangement cannot readily produce the PHI in the electronic form or format I requested, the Arrangement will provide either:

- electronic records in a form and format agreed to between the Arrangement and me; or
- a paper copy if I do not agree to any of the electronic formats offered by the Arrangement.

Check any of the below, as applicable:

_____ I want to inspect PHI about me maintained in the designated record set.

_____ I want to obtain a copy of PHI about me that is maintained in the designated record set.

_____ I want to inspect or obtain a copy of PHI about someone else that is maintained in the designated record set.

Name and birthdate of other individual: _____

My relationship to the individual is: _____

_____ I request that a copy of the requested PHI that is maintained in the designated record set be mailed to me at the following address:

_____

_____

_____ I request that a copy of the requested PHI that is maintained in the designated record set be mailed to the designated person at the following address:

Name of designated person: _____

Address: _____

I understand that the Arrangement will send PHI to another person designated by me only if my request is in writing, signed by me, and clearly identifies the designated person and where to send the copy of the PHI.

_____ I request that the information be sent to me by **unencrypted** email at the following email address: _____

Warning: It is possible that unauthorized third parties could read or access PHI sent by unencrypted email if they are able to intercept the transmission. If you still wish to receive PHI by unencrypted email, sign here to indicate your acceptance of this risk:

_____

I do/do not **(circle one)** agree that the Arrangement may provide a summary of the health information instead of allowing me to review the information.

II. Other Important Information

I understand that the Arrangement's Claims Administrator will fulfill this request and has 30 days to respond to this request. However, if the Arrangement is unable to take action within the initial 30-day period, then the Arrangement may extend the time for such action by an additional 30 days, provided that the Arrangement, within the first 30-day period, gives me a written statement of the reasons for the delay and the date by which the Arrangement will complete its action on the request.

I understand that if the Arrangement grants this request, in whole or in part, then it will inform me of the acceptance of this request and provide appropriate access. I understand that the Arrangement may need to follow up with me about a mutually convenient time and place for me to copy the requested PHI, or about a mutually agreeable form and format for electronic copies if the Arrangement cannot readily produce the PHI in my requested electronic form and format. If this is an inspection request, the Arrangement will arrange a mutually convenient time and place for me to inspect the requested PHI. However, if the Arrangement denies the request, in whole or in part, as permitted by HIPAA, it will provide me with a written denial.

If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the Arrangement will produce the PHI only once in response to a request.

I agree to pay any fees permitted by law for providing access, copies, summaries, and/or explanations of the requested PHI. Fees will be reasonable and cost-based and will include only the cost of labor for copying, supplies for creating the paper copy or electronic media for providing an electronic copy, postage (if I request that a copy or summary be mailed), and preparation of a summary (if I agree to a summary).

I understand that this request does not apply to certain health information, including (1) information that is not held in a designated record set; (2) psychotherapy notes; (3) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and (4) other health information not subject to the right to access information under HIPAA.

III. Signature of Individual or Individual's Representative

_____
Name

_____
Street Address

_____
City, State and Zip Code

_____
Telephone

_____
Email Address

I agree to pay any fees for copying, summarizing, or explaining my PHI. The fees will be reasonable and cost-based, and include only the cost of copying, postage, and the like. I understand that this request does not apply to certain health information, including: (1) information that is not held by the Arrangement; (2) psychotherapy notes; (3) information that was gathered in anticipation of a civil, criminal or administrative action or proceeding; and (4) other health information that is not subject to or is required to be disclosed under HIPAA.

_____	_____
Person's Signature	Date
_____	_____
Person's Printed Name	Date of Birth

If the Person's Representative is signing, the Representative must include a fully completed and signed Designation of Authorized Representative Form.

The request of the Claims Administrator should be mailed to:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT F – Sample Response to Request to Inspect or Copy Protected Health Information

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") is subject to the privacy rules under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"). HIPAA provides that a person may inspect and/or copy his or her protected health information ("PHI"). This is in response to such a request.

Date: _____

Name of Requesting individual: _____

The Arrangement received your request to access health information on [____date____].

I. Grant of Request

_____ Your request to access health information has been granted in its entirety.

_____ Your request to access health information has been granted in part. (*See the section entitled* "Denial of Access" *for an explanation regarding that portion of your access request that has been denied.*)

Access will be provided as follows:

_____ The Arrangement will provide you with access. Please contact Mark Hren, 9555 Rockside Road Cleveland, OH 44125, service@consoliplex.com to arrange a convenient time to copy and/or inspect the health information.

_____ A copy of the PHI will be provided in the electronic form and format you requested, and it will be forwarded to you pursuant to your prior instructions. **Note**, if you have requested that the Arrangement send PHI by unencrypted email, be aware, there is a risk that the email may be compromised during transmission. You previously indicated you are willing to accept the risk.

_____ The Arrangement cannot readily produce the electronic form or format you requested. Instead, the Arrangement will contact you to attempt to agree upon an alternate electronic form and format. If we cannot agree on a form and format, the Arrangement will provide you with a paper copy of the requested health information.

_____ A summary has been created based on the advance agreement provided by you.

_____ In accordance with your prior agreement, you must pay the Arrangement the following fees: [$_____]. The fees may relate to any of the following, as applicable: (1) the cost of labor for copying; (2) supplies for paper copies or electronic media; (3) postage; and (4) cost of preparation of an explanation of health information and/or summary of health information. These fees are reasonable in amount and cost-based, as permitted by law.

II. Need for Extension of Time

The Arrangement is reviewing your request to access health information, but the Arrangement needs additional time to determine if the requested access should be granted. A delay in responding to your request is necessary for the following reason(s):_____

_____

_____

The Arrangement anticipates a response to your request by [_____] [insert date for response deadline].

III. Denial of Access

Your request to access your health information is denied, in whole or in part, for the following reason(s):_____

_____

_____

If your request was denied in part, the Arrangement will give you access to other PHI requested, after excluding the information for which the Arrangement has denied access, as set forth in the section entitled "Grant of Request."

This denial ___ *is* ____ *is not* subject to appeal. You are entitled to an appeal if access was denied because (1) in the opinion of a licensed health care professional, granting access is likely to endanger the life or physical safety of your or another person; (2) the PHI makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or (3) the request for access was made by your personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to you or another person. In these cases, if you appeal, then your appeal will be reviewed by a licensed health care professional, designated by the Arrangement, who did not participate in the original decision. The appeal and notice of appeal decision will be conducted promptly. Following review of the appeal, the Arrangement will provide or deny access in accordance with the determination of the reviewing official. Any appeal must be in writing and submitted to the following address:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125

For questions, please contact the Privacy Officer at Service@consoliplex.com.

IV. Complaint Procedures

You may file a complaint regarding this decision with the Arrangement by filing it in writing with the following person: Privacy Officer at the above-listed address. Your complaint should include the reason(s) for the complaint, the grounds for disagreement with the Arrangement's decision to deny your requested access, and any other relevant information.

Alternatively, you may file a complaint with the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services. A complaint filed with OCR must: (1) be filed in writing, either on paper or electronically, and be submitted by mail, fax, or email; (2) name the plan that is the subject of the complaint and describe the acts or omissions believed to be in violation if HIPAA; and (3) be filed within 180 days after you receive notice of the denial of access. If you send the complaint by mail, send it to OCR's regional office where the alleged violation took place. You can find a list of regional offices, and information about filing a complaint electronically, on OCR's web site at http://www.hhs.gov/ocr/privacy/hipaa/complaints/.

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT G – Sample Request to Amend or Correct Protected Health Information

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") is subject to the privacy rules under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA").

HIPAA provides that a person may request the Arrangement amend or correct his or her protected health information ("PHI") under certain circumstances. However, HIPAA does not require the Arrangement to comply with the person's request. You may use this form to request the Arrangement amend or correct your "protected health information" but the Arrangement is not required to honor your request.

I. Request for Amendment or Correction

I request an amendment to protected health information ("PHI") about me in a "designated record set" (defined below) held by the Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") in accordance with administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and its implementing regulations. A *"designated record set"* is a group of records maintained by or for the Arrangement including enrollment, payment, claims adjudication, and health plan case or medical management record systems; or records used by or for the Arrangement to make decisions about individuals. The term "record" means any item, collection, or grouping of information that includes PHI that is maintained, collected, used, or disseminated by or for the Arrangement.

Describe Amendment Requested: _____

_____

_____

Reason for Requested Amendment: _____

_____

_____

I understand that the Arrangement will respond to my request within 60 days. The Arrangement will accept my request, deny my request, or notify me that it needs additional time (up to 30 days) to act on my request. If the Arrangement needs additional time, it will provide me with a written statement of the reasons why it needs more time and the date by which it will complete its action on the request.

If the Arrangement accepts the requested amendment, then the Arrangement shall: (A) make the appropriate amendment to the PHI; (B) inform me that my amendment request has been

accepted; and (C) request that I identify persons with whom the amendment needs to be shared as provided in HIPAA. The Arrangement shall make reasonable efforts to inform persons whom I identified. In addition, the Arrangement will notify other persons, including business associates of the Arrangement, that the Arrangement knows may have relied, or could foreseeably rely, on the information.

If the request is denied in whole or in part, then the Arrangement will provide me with a written denial notice describing the basis for the denial and my rights with respect to the denial.

II. Signature of Individual or Individual's Personal Representative

This request must be submitted to:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

Person's Signature	Date
Person's Printed Name	Date of Birth

If signed by Authorized Representative:

Authorized Representative

Relationship to Individual

If the Person's Representative is signing, the Representative must include a fully completed and signed Designation of Authorized Representative Form.

This request must be completed and submitted to the Privacy Officer at the following address:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT H – Sample Response to Request to Amend or Correct Protected Health Information

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") is subject to the privacy rules under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"). HIPAA provides that a person may request the Arrangement amend or correct their protected health information under certain circumstances. You have filed a request to have your PHI amended and/or corrected and this is the response to your request.

Date: _____

Name of Requesting Individual: _____

The Arrangement received your request on _____[date]_____.

I. Grant of Request

_____ Your request to amend or correct your PHI has been granted. The Arrangement will make an appropriate amendment to your PHI in a designated record set.

Please provide the Arrangement with the names of any persons who should receive the amended records. The Arrangement will make reasonable efforts to inform: (A) persons you identify; and (B) persons that the Arrangement knows may have relied, or could foreseeably rely, on records.

II. Need for Extension of Time

_____ The Arrangement is reviewing your request, but requires additional time to take action for the following reason(s):_____

_____

The Arrangement will respond to your request by _____. [insert date or time period not to exceed 30 additional days.]

III. Denial of Request

_____ Your request is denied for the following reason(s): _____

_____

_____

You have the right to file a written statement disagreeing with this denial of amendment. The statement of disagreement must be filed within 60 days of this notice with the following office: Mark Hren, Southern Ohio Chamber Alliance Benefit Plan Trust, c/o Consoliplex, 9555

Rockside Road Cleveland, OH 44125, service@consoliplex.com. The Arrangement may reasonably limit the length of your statement of disagreement. The Arrangement has the right to prepare a written rebuttal to your statement of disagreement. If the Arrangement prepares a rebuttal, you will receive a copy.

The Arrangement, as appropriate, shall identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link your request for an amendment, the Arrangement's denial of the request, your statement of disagreement, if any, and the Arrangement's rebuttal, if any, to the designated record set.

If you submit a statement of disagreement, then the Arrangement will include, with any subsequent disclosure of PHI to which the disagreement relates, the above-referenced material, or, at the Arrangement's election, an accurate summary of such information. If you do not submit a written statement of disagreement, you may ask the Arrangement to include your request for amendment and its denial, or an accurate summary, with any subsequent disclosure of the PHI, and the Arrangement will include that information with subsequent disclosures.

You may file a complaint regarding this decision with the following person: Mark Hren, 9555 Rockside Road, Cleveland OH 44125 at (216) 202-3499, or service@consoliplex.com. Your complaint should include the reason(s) for the complaint, the grounds for disagreement with the Arrangement's decision to deny your request, and any other relevant information.

Alternatively, you may file a complaint with the Secretary of the U.S. Department of Health and Human Services. It should be addressed as follows: The Hubert H. Humphrey Building, 200 Independence Avenue, S.W., Washington, D.C. 20201. A complaint filed with the Secretary must meet the following requirements: (A) it must be filed in writing, either in paper or electronically; (B) it must name the plan that is the subject of the complaint and describe the acts or omissions believed to be in violation of the HIPAA Privacy Standards; and (C) it must be filed within 180 days after receipt of this denial.

IV. Signature of Arrangement Representative

Name: _____

Signature: _____

Title: _____

Date: _____

If you have any questions or comments regarding this notice, please contact the Privacy Officer at the address or phone number listed above.

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT I – Sample Request for Restriction on Use or Disclosure of Protected Health Information

Name: _____

Date: _____

I. Request for Restriction

I understand that the Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") may use and disclose protected health information ("PHI") about me for purposes of treatment, payment, and health care operations without my authorization or opportunity to agree or object. I request that the Arrangement restrict use and disclosure of PHI regarding treatment, payment, and health care operations about me, or to restrict disclosures of my PHI to family members, relatives, friends, or other persons identified by me who are involved in my care or payment for that care, in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its regulations.

(a) I request that the restrictions apply to the following information: _____

_____

_____

(b) I request that the use and disclosure of the information described above be restricted in the following manner: _____

_____

_____

(c) I request that my PHI not be disclosed to the following individuals or entities:

_____

_____

I understand that the Arrangement is not required to agree to requested restrictions, with one exception. The Arrangement will agree to a request to restrict disclosure of my PHI to a health plan if: (A) the disclosure is for the purpose of carrying out payment or health care operations (i.e., not for treatment) and is not otherwise required by law; and (B) the PHI pertains solely to a health care item or service for which I, or someone (other than the Arrangement) acting on my behalf, has paid in full.

II. Other Important Information

I understand that if restricted PHI must be used or disclosed to provide emergency treatment for me, then this restriction is void. I understand that if the Arrangement agrees to a restriction, either the Arrangement or I may terminate this restriction at any time (except the Arrangement will not terminate any restriction that is required by law). If the Arrangement informs me that it is terminating its agreement to a restriction, the termination of the restriction is only effective with respect to PHI created or received after the Arrangement informs me of the termination.

I understand that if a restriction is agreed to by the Arrangement, it is not effective to prevent uses or disclosures required by the Secretary of the U.S. Department of Health and Human Services to investigate the Arrangement's compliance with HIPAA or uses or disclosures that are otherwise required by law.

I understand that if a restriction is not specifically listed above and agreed to in writing by the Arrangement, it will not be effective.

III. Signature of Individual or Individual's Personal Representative

Signature	Date
Printed Name	Date of Birth

If signed by individual's personal representative:

Printed name of the individual's personal representative:

Relationship to the individual, including authority for status as personal representative:

If the Person's Representative is signing, the Representative must include a fully completed and signed Designation of Authorized Representative Form.

This request must be completed and submitted to the Privacy Officer at the following address:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT J – Sample Response to Request for Restrictions on Use or Disclosure of Protected Health Information

Name: _____

Date: _____

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") received your request for restrictions on the use or disclosure of your protected health information ("PHI") on _____ _____ *[insert date of receipt]*.

I. Approval of Request

_____ Your request to restrict the use and disclosure of PHI has been granted in accordance with your request, subject to the following: [Include a description of how the requested restriction will be applied to minimize risk of misunderstandings. Agreed restrictions must be documented in accordance with 45 CFR §164.530(j).]

_____

_____

- You may terminate this restriction at any time.
- The Arrangement may terminate this restriction at any time, so long as the restriction is not required by law. If the Arrangement informs you that it is terminating the restriction, then the termination of the restriction is only effective with respect to PHI created or received after the Arrangement informs you of the termination.
- If restricted PHI must be used or disclosed to provide emergency treatment for you, then this restriction is void.
- The restriction is not effective to prevent uses or disclosures required by the Secretary of the U.S. Department of Health and Human Services to investigate the Arrangement's compliance with HIPAA or uses or disclosures that are otherwise required by law.
- If a restriction is not specifically listed on the request, it will not be effective.

II. Denial of Request

_____ Your request to restrict use and disclosure of PHI has been denied. See the Arrangement's Notice of Privacy Practices for more information about your rights. For a copy, contact:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

III. Signature of Arrangement Representative

_____
Name

_____
Signature

_____
Title

_____
Date

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT K – Sample Request for Alternate Communications

Name: _____

Date: _____

I. Request for Alternate Communications

I request that I receive communications of my protected health information ("PHI") from the Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") by the following alternative means or at the following alternative locations: _____

_____

_____

(Individual should specify alternative means (e.g., only by telephone) or alternative location (e.g., relative's mailing address).)

I request that the following communications be subject to the above request:

_____

Information for alternative means of contact (provide phone number or address to be used for communications subject to request): _____

_____

_____ **I certify that the disclosure of all or part of the information to which this request pertains could endanger me.**

II. Other Important Information

I understand that the Arrangement will agree to reasonable requests. The Arrangement may condition its accommodation or receiving (A) information as to how payment will be handled: and (B) sufficient information to allow necessary communications (such as an alternative address or method of contact).

III. Signature of Individual or Individual's Personal Representative

_____ _____

Signature Date

_____ _____

Printed Name Date of Birth

If signed by individual's personal representative:

Printed name of the individual's personal representative:

_____

Relationship to the individual, including authority for status as personal representative:

_____

If the Person's Representative is signing, the Representative must include a fully completed and signed Designation of Authorized Representative Form.

This request must be completed and submitted to the Privacy Officer at the following address:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT L – Sample Response to Request for Alternate Communications

Name: _____

Date: _____

The Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") received your request for alternative communications of your protected health information ("PHI") on _____ [insert date of receipt].

I. Approval of Request

_____ Your request for confidential communications of PHI has been granted in accordance with your request.

II. Need More Information

_____ Your request for confidential communications of PHI has been received; however, your request did not include the information indicated below. If you submit the following information, the Arrangement will review your request again: _____

_____

Please provide an alternative address or other method of contact: _____

_____

Please provide information on how Arrangement benefits should be paid: _____

_____

III. Denial of Request

_____ Your request for confidential communications of PHI has been denied for the following reason(s):_____

_____

_____

Note: The Arrangement is required to accommodate "reasonable" requests. If the Arrangement considers a request to be unreasonable, it should identify the unreasonable

aspects of the request. See the Arrangement's Notice of Privacy Practices for more information about your rights. For a copy, contact:

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

IV. Signature of Arrangement Representative

Name:_____

Signature:_____

Title:_____

Date:_____

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT M – Sample Summary Privacy Practices

I. Summary of Privacy Practices

This Summary of Privacy Practices summarizes how medical information about you may be used and disclosed by the Southern Ohio Chamber Alliance Benefit Plan (the "Arrangement") or others in the administration of your claims, and certain rights that you have. For a complete, detailed description of all privacy practices, as well as your legal rights, please refer to the accompanying Notice of Privacy Practices. This Summary is not intended to be a comprehensive statement of your privacy rights. In case of conflict between this Summary and the complete Notice, the Notice will be controlling.

You should contact the Privacy Officer for requests to inspect, copy, amend, or correct any Protected Health Information ("PHI"):

Privacy Officer
Southern Ohio Chamber Alliance Benefit Plan Trust
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

II. Our Pledge Regarding Medical Information

We are committed to protecting your personal health information. We are required by law to (1) make sure that any medical information that identifies you is kept private; (2) provide you with certain rights with respect to your medical information; (3) give you a notice of our legal duties and privacy practices; and (4) follow all privacy practices and procedures currently in effect.

Please note that the Arrangement's Board of Trustees and your Participating Employer do not, except in very rare, limited circumstances, have access to or maintain PHI.

III. How We May Use and Disclose Medical Information About You

We may use and disclose your personal health information without your permission to facilitate your medical treatment, for payment for any medical treatments, and for any other health care operation. We will disclose your medical information to specified employees of third parties who perform necessary plan administrative functions. We will disclose the minimum amount of information necessary for the specific function. If your Participating Employer ever should have access to PHI, your Participating Employer cannot use your information for employment-related purposes. We may also use and disclose your personal health information without your permission for the reasons stated in the Notice and as allowed or required by law. Otherwise, we must obtain your written authorization for any other use and disclosure of your medical

information. Neither the Arrangement nor your Participating Employer can retaliate against you if you refuse to sign an authorization or revoke an authorization you had previously given.

IV. Your Rights Regarding Your Medical Information

You have the right to inspect and copy your medical information, to request corrections of your medical information, and to obtain an accounting of certain disclosures of your medical information. You also have the right to request that additional restrictions or limitations be placed on the use or disclosure of your medical information, or that communications about your medical information be made in different ways or at different locations.

V. How to File a Complaint

If you believe your privacy rights have been violated, you have the right to file a complaint with us or with the U.S. Department of Health and Human Services, Office for Civil Rights. We will not retaliate against you if you file a complaint.

SOUTHERN OHIO CHAMBER ALLIANCE BENEFIT PLAN TRUST

HEALTH BENEFITS PLAN

EXHIBIT N – Sample Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW EACH PERSON ENROLLED IN THE PLAN CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

THE PARTICIPANT SHOULD CONTACT THE PRIVACY OFFICER FOR REQUESTS TO INSPECT, COPY, AMEND OR CORRECT ANY PROTECTED HEALTH INFORMATION. THE PRIVACY OFFICER WILL PROVIDE THE PARTICIPANT WITH THE INFORMATION REQUIRED TO FULFILL THE REQUEST.

Privacy Officer
c/o Consoliplex
9555 Rockside Road
Cleveland, OH 44125
Service@consoliplex.com

This notice describes the Southern Ohio Chamber Alliance Benefit Plan's (the "Arrangement") legal obligations and each Participant's legal rights with respect to the privacy of each Participant's protected medical and health information.

The Arrangement and each Participating Employer in the Arrangement are committed to keeping each Participant's medical and health information confidential and secure. Please note that except in very limited circumstances, your Participating Employer has no access to any Participant's Protected Health Information. In addition, the Arrangement is required by law to take reasonable steps to ensure each Participant's Protected Health Information ("PHI") as defined below, remains private.

The Arrangement collects a variety of medical and health information. The employee application form provides some of this information. Correspondence between the Arrangement and the individual may provide other information. Other information is provided in correspondence between the Arrangement and the individual. The Arrangement also receives health and medical information from others such as the person's physician, other medical providers and insurance companies.

The Arrangement treats all personal information securely and confidentially. The Arrangement limits access to this information to only those individuals who need this information to administer the Arrangement. These individuals are trained on how important it is to safeguard this information and they must comply with all applicable laws and the Arrangement's own procedures governing confidentiality. The Arrangement maintains strict physical, electronic and procedural security standards to protect personal information and the Arrangement also has established and maintains internal procedures to ensure the integrity and accuracy of such information.

The Arrangement is required by law to maintain the privacy of the person's PHI. The law also requires the Arrangement to provide individuals with notice of the Arrangement's legal duties and privacy practices with respect to PHI. Individuals that participate in the Arrangement may request the Privacy Officer for certain information as outlined below. The Arrangement is required to comply with the terms of this notice.

Each Participant enrolled in the Arrangement may request the Privacy Officer to inspect, copy, amend, or change their PHI. The person must complete the Authorization to Release PHI. This will be supplied by the Privacy Officer.

Each Participant may authorize a representative to view their PHI. The Participant must complete an Authorization for a Personal Representative supplied by the Privacy Officer.

The Privacy Officer, after reviewing the request's compliance with HIPAA will forward the PHI request to the Claims Administrator. The Claims Administrator will respond to the request for PHI in accordance with the rules and will forward the response to the Participant or the Authorized Representative.

PHI is defined as information that is created or received by the Arrangement and relates to the past, present or future physical or mental health or condition of a Participant; the provision of health care to a Participant; or the past, present or future payment for the provision of health care to a Participant; and that identifies the Participant or for which there is a reasonable basis to believe the information can be used to identify the Participant.

The Arrangement may use and disclose PHI in the following ways:

USES AND DISCLOSURES OF PHI

Uses and Disclosures for Payment

The Arrangement may use and disclose PHI about you to determine your eligibility for plan benefits and to pay claims for the treatment and services you have received from various providers. The Arrangement has delegated claims payment and any appeal of claim determinations to the Claims Administrator. The Arrangement's Board of Trustees and the Participating Employer do not have access to PHI. The Claims Administrator may use and disclose your PHI to coordinate Arrangement coverage and determine benefit responsibility. For example, the Claims Administrator may disclose your PHI to your health care provider regarding your medical history to determine if a particular treatment is experimental, investigational or medically necessary or to determine if the treatment or services are covered under the Arrangement. The Claims Administrator also may use your PHI for utilization review or precertification. Additionally, the Claims Administrator may forward PHI to another entity to help process and pay claims, coordinate and/or subrogate benefits and claims.

Uses and Disclosure for Treatment

The Claims Administrator may use and disclose PHI about you to facilitate medical treatment or services by various providers who are involved with your care. For example, the Claims Administrator may disclose prior treatments and prescriptions so that the provider may provide

appropriate care to you. The Claims Administrator also may use your PHI to advise you about alternative treatments and other health related information that may help you.

Uses and Disclosures for Health Care Operations

The Arrangement may allow service providers to use and disclose PHI about you for other the Arrangement operations. These uses and disclosures are necessary to operate the Arrangement. For example, the Claims Administrator may use medical information to perform quality assessment and improvement activities, underwriting, premium rating and other activities relating to the Arrangement coverage. The Arrangement also may allow service providers the use of your PHI when submitting claims for stop loss coverage, when conducting medical reviews, obtaining legal and auditing services. In addition, your PHI may be used to help detect fraud and abuse as well as being used for business planning and development such as cost and business management and general the Arrangement administrative activities. However, the Arrangement will not use or disclose genetic information for underwriting purposes.

Uses and Disclosures Required by Law

The Arrangement will direct and allow your PHI to be provided by the Claims Administrator when required by Federal, State or Local law. For example, the Arrangement will allow your PHI to be provided by the Claims Administrator when required by court order or in a lawsuit involving medical malpractice.

Uses and Disclosures to Avert Serious Threat to Health and Safety

The Claims Administrator may use and disclose your PHI to prevent a serious threat to your health and safety or the health and safety of the public or another person. Such use and disclosure would be to someone able to help prevent the threat. For example, the Claims Administrator may disclose PHI in a licensing proceeding for a physician.

OTHER SITUATIONS

Disclosure to Another Plan

Your PHI may be disclosed by the Claims Administrator to another health plan. This disclosure may help facilitate the payment of claims under that other health plan. The PHI also may be disclosed to certain individuals or entities so that they can administer another plan.

Disclosure to Family and Friends Involved In Your Care

The Arrangement may, with your approval, direct disclosure, from time to time, of your personal health information to designated family, friends and others who are involved in your care or in payment for your care to help facilitate that person's involvement in caring for you or paying for your care. If you are unavailable, incapacitated or have an emergency medical situation and the Arrangement determines that limited disclosure maybe in your best interest, the Arrangement may direct the Claims Administrator to share limited personal health information with such individuals without your approval. The Arrangement may also direct disclosure of limited personal health information to a public or private entity that is authorized to assist in disaster relief efforts so that entity can locate a family member or other person that may be involved in some aspect of caring for you.

Disclosure to Business Associates

The Arrangement may contract with various other entities called Business Associates to help administer the Arrangement and perform various functions for the Arrangement. The Arrangement may share your PHI with these Business Associates but only after the Business Associates has agreed, in writing, to protect and safeguard your PHI. The Claims Administrator is one example of a Business Associate.

Disclosure for Organ and Tissue Donations

If you are an organ or tissue donor the Arrangement may direct the Claims Administrator to release your PHI to organizations that handle organ and tissue procurement or transplants.

Disclosure for Military and Veterans

If you are in the armed forces the Arrangement may direct the Claims Administrator to release or disclose your PHI as required by the military command.

Disclosure for Workers' Compensation

The Arrangement may direct the Claims Administrator to release or disclose your PHI for workers' compensation and similar programs that provide benefits for work related injuries and illness.

Disclosure of Public Health Risks

The Arrangement may direct the Claims Administrator to release or disclose your PHI for public health activities. These activities include:

1. To prevent or control disease, injury, or disability;

2. To report deaths and births;

3. To report child abuse or neglect;

4. To report reactions to medications or problems with products;

5. To notify individuals or product recalls;

6. To disclose immunization information to schools if required by state law;

7. To notify an individual who may have been exposed to a disease or may be at risk for contracting or spreading a disease;

8. To notify the appropriate authorities if there is reason to believe a person has been the victim of abuse, neglect or domestic violence. This type of disclosure will only be made if the person agrees to the disclosure or when the disclosure is required by law.

Disclosure for Health Oversight Activities

The Arrangement may direct the Claims Administrator to release or disclose your PHI to a health oversight agency as authorized by law. The disclosure is necessary for the government

to monitor health care systems, government programs and compliance with various laws. The PHI may be used for audits, investigations, inspections and licensure.

Disclosures for Lawsuits and Other Disputes

If you are involved in a lawsuit or other type of dispute the Arrangement may direct the Claims Administrator to release or may disclose PHI in response to a court or administrative order. The PHI also may be disclosed in response to a subpoena, discovery request or any other lawful process by someone involved in the lawsuit or dispute. However, that will only occur if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Disclosure for Law Enforcement

The Arrangement may direct the Claims Administrator to release PHI if requested by a law enforcement official:

1. In response to a court order, subpoena, warrant, summons or similar process;

2. To identify a crime victim if, under certain circumstances, the Arrangement is unable to obtain the person's consent;

3. Disclosure to report a death if criminal activity is suspected;

4. Disclosure if criminal activity is suspected with a medical provider; and

5. In an emergency to report a crime, the location of the victim(s) or to help identify the person who may have committed the crime.

Disclosure to Medical Examiners

The Arrangement may direct the Claims Administrator to release or disclose PHI to a coroner, medical examiner, funeral director so that they may carry out their duties such as identifying the person or determining the cause of death.

Disclosures for Miscellaneous Reasons

The Arrangement may direct the Claims Administrator to release or disclose PHI for national security reasons as required by law or for other reasons like providing information for the treatment of inmates.

No Other Disclosures

The Arrangement will not use or disclose PHI for marketing or fundraising purposes without your prior written authorization. In addition, the Arrangement will not disclose your PHI for any other reason without your prior written authorization and you may revoke that authorization on a prospective basis at any time.

YOUR RIGHTS REGARDING YOUR PHI

You have the following rights with respect to your PHI.

Right to Inspect and Copy

You have the right to inspect and copy your PHI held by the Arrangement. If your PHI is maintained in electronic format, you have the right to receive that PHI in an electronic format that you and the Arrangement agree on. All requests must be in writing on an approved form and must be submitted to the Privacy Officer at the address listed below. The Arrangement will respond to your request within sixty days by directing the request to the Claims Administrator. The Claims Administrator may request up to an additional thirty days to gather the information.

There may be a charge associated for copying, mailing, etc. your PHI.

Under certain limited circumstances your request to review and copy your PHI may be denied. For example, the law states an individual does not have the right to review and copy psychotherapy notes and information compiled in anticipation of a lawsuit. If your request is denied, you will be notified, in writing, why the request was denied, how you can appeal the decision and a copy of the Arrangement's complaint procedures.

Right to Amend or Correct

If you believe the Arrangement's Claims Administrator's medical information about you is not correct or is incomplete, you may ask the Claims Administrator or your health care service provider to amend or correct the information by contacting the Privacy Officer, in writing, and stating why you believe the information should be amended. The Privacy Officer may deny your request to amend the information if you do not state why you want the information amended or if you refuse to supply the Arrangement with information it needs to determine if the amendment should be made. In addition, the Arrangement may refuse to amend the information if:

1. the information is not part of the Arrangement's medical information;

2. the information was not created by the Arrangement unless the person or entity that created the information is no longer available to make the amendment;

3. the information is not part of the information which you are permitted to inspect and copy; or

4. the information is complete and accurate.

You have the right to request the Claims Administrator or your health care service provider to amend your medical information for as long as they maintain that information. The Arrangement will respond to your request to amend your PHI within sixty days unless the Arrangement requests an additional thirty days to respond to your request.

If your request is denied, you will be notified, in writing, why the request was denied, how you can appeal the decision and a copy of the Arrangement's complaint procedures.

Right to an Accounting

You have the right to request an accounting of certain disclosures of your PHI. Your request must be in writing on an approved form and must be submitted to the Privacy Officer. The request must state the time period that cannot be before January 1st 2015 and cannot be for more than six years. You must identify the format (i.e., paper or electronic) in which you want

the information. If you request this information within twelve months of a previous request, the Arrangement may charge to process your request.

The Arrangement is not required to provide you an accounting of disclosures that were made for purposes of treatment, payment or health care operations.

The Arrangement will respond to your request within sixty days unless the Arrangement requests an additional thirty days to respond to your request. If your request is denied, you will be notified, in writing, why the request was denied, how you can appeal the decision and a copy of the Arrangement's complaint procedures.

Right to Request Restrictions

You have the right to request the Arrangement place restrictions or limitations on your PHI use or discloses for treatment, payment or health care operations. You also have the right to request a limit on the medical information disclosed to someone who is involved with your care or payment for your care, like a family member or friend. If you would like to restrict or limit the disclosure of your PHI, you must submit a request to the Privacy Officer on an approved form. You must list:

1. what information you want limited,

2. whether you want to limit the use and disclosure of the information, and

3. who you want the restrictions to apply to (e.g., a spouse).

Please note that the Arrangement is not required to honor your request to limit or restrict the use or disclosure of your PHI.

Right to Notification

You have the right to be notified if there is a breach of your unsecure PHI and the Arrangement will notify you of such breach in a timely manner that complies with all applicable statues and rules.

Right to Request Confidential Communications

You have the right to request that all communications regarding your PHI be in a certain format or be at a certain location. For example, you may request that the communication be mailed to your work. To request a confidential communication, you must submit your request on an approved form to the Privacy Officer. The Arrangement will accommodate all reasonable requests and the Arrangement will not ask why you are making the request.

Right to a Paper Copy of this Notice

You are entitled to a paper copy of this notice at any time. To request a copy of this notice, please contact the Privacy Officer.

Rights Regarding Personal Representatives

You may exercise any of your rights listed in this notice through a personal representative. You must designate your personal representative on an approved form that you can obtain from the

Privacy Officer. The Arrangement retains the right to deny access of your PHI to your personal representative if the Arrangement determines it is in your best interest not to disclose the information.

CHANGES TO THIS NOTICE

This Privacy Notice is effective January 1st, 2015. However, the Arrangement reserves the right to modify this notice at any time (even retroactively) with respect to medical information it already has as well any medical information it may receive in the future. The Arrangement will provide Participants with any revised notice annually. This notice is intended to comply with the privacy rights under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and should be interpreted accordingly. This notice is not intended to give anyone any greater rights than those required under HIPAA.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with the Privacy Officer.

You also may file a complaint with the U.S. Department of Health and Human Services if you believe your privacy rights have been violated. You can obtain a copy of the complaint form from the Privacy Officer, or you may obtain a copy of the form from the Office of Civil Rights at the U.S. Department of Health and Human Services over the internet at http://www.hhs.gov/ocr/HIPAA.

Complaints may be filed with the Office of Civil Rights at the U.S. Department of Health and Human Services at the following e-mail address: mail to: OCRComplaint@hhs.gov.

Alternatively, you can file the complaint by mail or fax at the following address:

Office for Civil Rights
Centralized Case Management Operations
Department of Health and Human Services
Independence Avenue, S.W.
Room 509F HHH Bldg.
Washington, D.C. 20201

All complaints should identify the Arrangement and list the acts or omissions that you believe violate your privacy rights. The complaint must be filed with the Office of Civil Rights at the above address within 180 days of the date you knew or should have known of the alleged violation. The government may waive the 180-day filing deadline if you can show good cause why you failed to file the complaint in time.

The Arrangement and the Participating Employer will not retaliate against anyone who files a complaint with the Privacy Officer and/or the Office of Civil Rights at the U.S. Department of Health and Human Services. In addition, the Arrangement will never ask you to waive your rights under HIPAA.