TRINITY UNIVERSITY GROUP HEALTH PLAN

TRINITY UNIVERSITY FLEXIBLE BENEFIT PLAN

HIPAA POLICY AND PROCEDURES
# TABLE OF CONTENTS

## GENERAL
Definitions .................................................................................................................................................. 1  
Policies And Procedures ............................................................................................................................... 3  

## BUSINESS ASSOCIATE AGREEMENTS
Business Associate Agreements—Core Policy ............................................................................................. 4  
Business Associate Agreements—Compliance .............................................................................................. 5  
Business Associate Agreements—Uses And Disclosures ........................................................................... 7  
Business Associate Agreements—Document Retention ............................................................................... 8  

## DATA USE
Data Use—De-Identified Information ........................................................................................................... 9  
Data Use—Limited Data Sets ..................................................................................................................... 11  

## VERIFICATION
Verification ..................................................................................................................................................... 13  

## DOCUMENT RETENTION
Document Retention ..................................................................................................................................... 16  

## PRIVACY

### ADMINISTRATIVE REQUIREMENTS
Privacy Officer .................................................................................................................................................. 18  
Contact Office .............................................................................................................................................. 20  
Privacy Workers .......................................................................................................................................... 21  
Training ....................................................................................................................................................... 22  
Form: Occurrence of HIPAA Privacy Training .............................................................................................. 23

---

4817-6164-6114.4
Form: Acknowledgment of HIPAA Privacy Training .................................................. 24
Complaints ................................................................................................................... 25
Sanctions ...................................................................................................................... 27
Form: Report of Complaint Investigation ................................................................. 29
Mitigation ..................................................................................................................... 30
No Retaliation or Intimidation .................................................................................... 31
No Waiver of Rights .................................................................................................... 32

AUTHORIZATIONS
Authorizations—Core Policies .................................................................................. 33
Authorizations—Psychotherapy Notes ..................................................................... 36
Authorizations—Requested by a Participant or by the Plan ........................................ 35
Authorizations—Received from Another .................................................................... 37
Authorizations—Revocation ....................................................................................... 38
Authorizations—Using or Disclosing PHI Accordingly ............................................. 39
Authorizations—Document Retention ...................................................................... 40
Form: Authorization .................................................................................................. 41
Checklist: Validating Authorizations ........................................................................ 44

MINIMUM NECESSARY
Minimum Necessary—Core Policies ......................................................................... 46
Minimum Necessary—Uses and Disclosures of PHI .................................................. 47
Minimum Necessary—Requesting PHI ....................................................................... 48
Minimum Necessary—Responding to a Request for PHI ........................................... 49
Minimum Necessary—Document Retention ................................................................. 51

INDIVIDUAL RIGHTS
Right to Notice of Privacy Practices ........................................................................... 52
Right to Request Restrictions ...................................................................................... 55
Form: Request for Restrictions ................................................................................... 58
Form: Granting or Denying a Request for Restriction ................................................. 59
Request for Confidential Communication .................................................................... 60
Form: Request For Confidential Communication ..................................................... 62
USES AND DISCLOSURES

HITECH

Prohibition on Sale of PHI

Breach Notification of Unsecured PHI
SECURITY

ADMINISTRATIVE SAFEGUARDS

Assigned Security Responsibility ................................................................. 115
Risk Analysis .................................................................................................. 118
Risk Management .......................................................................................... 120
Sanctions ......................................................................................................... 121
Form: Sanction Log ....................................................................................... 122
Information System Activity Review .............................................................. 123
Workforce Security ......................................................................................... 124
Form: Termination-Of-Access Checklist ......................................................... 126
Information Access Management .................................................................. 127
Security Awareness and Training ................................................................. 128
Form: Training Log ....................................................................................... 131
Security Incidents ......................................................................................... 132
Form: Security Incident Report ..................................................................... 133
Form: Security Incident Log .......................................................................... 134
Contingency Plan .......................................................................................... 135
Evaluation ...................................................................................................... 137

PHYSICAL SAFEGUARDS

Facility Access Controls .............................................................................. 138
Form: Visitor Access Log ............................................................................. 140
Form: Special Access Log ............................................................................ 141
Form: Maintenance Log .............................................................................. 142
Workstation Use and Security ...................................................................... 143
Device and Media Controls .......................................................................... 146
TECHNICAL SAFEGUARDS

Technical Access Control ........................................................................................................... 148
Audit Controls.................................................................................................................................. 150
Integrity.......................................................................................................................................... 151
Person or Entity Authentication..................................................................................................... 152
Transmission Security.................................................................................................................. 153
As used in these HIPAA Policies and Procedures, *italicized* terms have the meaning that is set forth in the Rule. The following capitalized terms have the following definitions.

“Facility” generally means the building(s) housing the information systems containing the Plan’s electronic PHI. The term “Facility” is limited to building(s) under the control of the Plan Sponsor. For purposes of these HIPAA Policies and Procedures, “Facility” means One Trinity Place, San Antonio, TX 78212-7200.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996, as amended.

“HIPAA Breach” means any unauthorized acquisition, access, *use*, or *disclosure* of Unsecured PHI, unless the Plan demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI was mitigated.

A HIPAA Breach does not occur:

- Due to the inadvertent acquisition, access, or *use* by an *individual* acting under the authority of the Plan (or one of its *business associates*), provided that
  - Such acquisition, access, or *use* was made in good faith and within the course and scope of the professional relationship between such *individual* and the Plan or its *business associate*; and
  - such information is not further acquired, accessed, *used*, or *disclosed* by any person;
- Due to the inadvertent *disclosure* by a person who is otherwise authorized to access PHI at a Facility operated by the Plan (or one of its *business associates*) to another similarly situated person at the same Facility, provided that any such information is not further acquired, accessed, *used*, or *disclosed* without authorization.
- If the Plan (or its *business associate*) reasonably believes that the unauthorized person
to whom the *PHI* was *disclosed* would not reasonably have been able to retain such information.

“**Location**” generally means the room(s) or floor(s), within a Facility, housing the information systems containing the Plan’s *electronic PHI*. For purposes of these HIPAA Policies and Procedures, “Location” means Human Resources, Northrup Hall Room 210.

“**Plan**” means the Trinity University Group Health Plan and the component health plans of the Trinity University Flexible Benefit Plan.

“**Plan Sponsor**” means Trinity University.

“**Privacy Workers**” means the designated Workforce Members who are permitted, under the Plan, HIPAA, and these HIPAA Policies and Procedures, to access, *use*, and *disclose* the *PHI* that is within the Plan’s control.

“**Rule**” means the regulations implementing HIPAA’s privacy and security provisions, namely 45 CFR Parts 160 through 164.

“**Unsecured PHI**” means *PHI* that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the *Secretary*.

“**Workforce Members**” means employees, volunteers, trainees, temporary staff and other persons, including independent contractors, whose conduct, in the performance of work for Plan Sponsor, is under the direct control of Plan Sponsor, whether or not they are paid by Plan Sponsor.
POLICIES AND PROCEDURES

Section: General                      Effective Date: June 1, 2008
Subsection: n/a                    Last Reviewed On: September 23, 2013

POLICY

The Plan will adopt and implement written HIPAA Policies and Procedures, which will be designed to comply with the Rule. Only the Vice President Finance & Administration, Assistant Vice President Human Resources, Associate Director Human Resources, Employment & Benefits Administrator, Human Resources Coordinator, Human Resources Assistant, Security Administrator, and the Benefits Committee shall have the right to amend or alter these HIPAA Policies and Procedures. The Vice President Finance & Administration, Assistant Vice President Human Resources, Associate Director Human Resources, Employment & Benefits Administrator, Human Resources Coordinator, Human Resources Assistant, Security Administrator, and the Benefits Committee are encouraged, but not required, to seek the advice of the Privacy Officer, Security Officer and/or legal counsel before making any such amendments or alterations.

PROCEDURE

All policies and procedures shall be forwarded to the Privacy Officer, who shall maintain a copy of these HIPAA Policies and Procedures in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.

All Privacy Workers shall comply with these HIPAA Policies and Procedures. If a Privacy Worker has any doubt as to whether a use or disclosure is authorized by the Rule or by these HIPAA Policies and Procedures, the Privacy Worker should consult with the Privacy Officer or HIPAA counsel.

Upon a material change to HIPAA or to the Rule, the Plan shall promptly revise these HIPAA Policies and Procedures to comply with the change, implement the revisions, and retrain Privacy Workers as necessary.

If the Plan revises these HIPAA Policies and Procedures, and if the revision materially affects the Plan’s Notice of Privacy Practices (a “material revision”), the Plan shall make a corresponding revision to the Notice of Privacy Practices.
# BUSINESS ASSOCIATE AGREEMENTS—CORE POLICY

<table>
<thead>
<tr>
<th>Section: General Subsection: Business Associate Agreements</th>
<th>Effective Date: June 1, 2008 Last Reviewed On: September 23, 2013</th>
</tr>
</thead>
</table>

## POLICY

In order to disclose PHI to a business associate, the Plan shall first have in place a written and HIPAA-compliant business associate agreement.

## PROCEDURE

A business associate is a person or entity who provides certain functions, activities, or services for or on behalf of the Plan which involve the use and/or disclosure of PHI and who is not an employee of the Plan.

To the extent possible, the Plan shall use a standardized business associate agreement. The Plan's form business associate agreement shall contain all of the elements required by the Rule.

The Plan’s form business associate agreement shall require business associate agreements between the business associate and its subcontractors to comply with the same requirements that apply to agreements between a covered entity and a business associate. In addition, the business associate agreement will provide that the business associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that the business associate creates, receives, maintains or transmits on behalf of the Plan as required by the Rule. Further, the business associate shall ensure that any agent, including a subcontractor, to whom the business associate provides such information, agrees to implement reasonable and appropriate safeguards to protect electronic PHI. The business associate must timely report to the Plan and the Security Officer any security incident of which it becomes aware.

The business associate agreement required by this Policy may be a separate document, may be an addendum to a document, or may be incorporated into a larger agreement.

Requests for business associate agreements shall be directed to the Privacy Officer.

The Privacy Officer shall perform an internal audit, periodically, to ensure that the Plan has accurately identified, and has a signed business associate agreement with, its business associates.
BUSINESS ASSOCIATE AGREEMENTS—COMPLIANCE

<table>
<thead>
<tr>
<th>Section: General</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Business Associate Agreements</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

The Plan shall comply with the terms of any *business associate* agreement to which it is a party, and will insist upon compliance by the *business associate*.

**PROCEDURE**

*Suspected Breach of Business Associate Agreement*

If any Workforce Member suspects that any party to one of the Plan’s *business associate* agreements has breached the *business associate* agreement, that Workforce Member shall immediately report the suspected breach to the Privacy Officer.

The suspected breach shall be investigated by the Privacy Officer. The Privacy Officer shall document the results of the investigation.

If the investigation reveals that the breach was not material and was not a HIPAA Breach, the Privacy Officer shall take such other steps as may be required under other policies, where applicable, such as the Sanctions Policy and the Mitigation Policy.

In addition, if applicable, the Privacy Officer shall recommend that the Plan reconsider, revise, or supplement these HIPAA Policies and Procedures to reduce the likelihood of a similar breach in the future.

*HIPAA Breach*

If the investigation reveals a HIPAA Breach, whether by the *business associate* or the Plan, the Privacy Officer shall implement the procedures set forth for a Breach of *Unsecured PHI*.

A *business associate* shall be required, following the discovery of a HIPAA Breach, to provide notification to the Plan without unreasonable delay and in no case later than sixty (60) days after the discovery. A *business associate* shall be deemed to have knowledge of a HIPAA Breach if the HIPAA Breach is known, or by exercising reasonable diligence, would have been known, to any person, other than the person committing the HIPAA Breach, who is an employee, officer, or other agent of the *business associate*.

The notification shall include, to the extent possible, the identification of each *individual* whose *Unsecured PHI* has been, or is reasonably believed by the *business associate* to have been accessed, acquired, *used* or *disclosed* during the HIPAA Breach. The *business associate* shall be required to provide the Plan with any other information that the Plan is required to include in the
notification to *individuals*.

**Material Breach**

If the investigation reveals a material breach by the *business associate*, then depending upon the circumstances and the rights set forth in the *business associate* agreement, the Plan may take one or more of the following actions:

- If the breach is curable, the Plan may provide an opportunity for the *business associate* to cure the breach or end the violation.

- If the *business associate* fails to cure the breach or end the violation, the Plan may terminate the *business associate* agreement.

If the investigation reveals a material breach by the Plan, Privacy Officer shall take such other steps as may be required under other policies, such as the Sanctions Policy or the Mitigation Policy. If the breach involves *Unsecured PHI*, then the Privacy Officer shall follow the Plan’s HIPAA Breach Notification Policy and Procedure.

If applicable, the Privacy Officer shall recommend that the Plan reconsider, revise, or supplement these HIPAA Policies and Procedures to reduce the likelihood of a similar breach in the future.
BUSINESS ASSOCIATE AGREEMENTS—USES AND DISCLOSURES

Section: General
Subsection: Business Associate Agreements
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan may disclose PHI to a business associate, provided that a business associate agreement is in place and further provided that the disclosure is consistent with these policies and procedures.

PROCEDURE

When the Plan discloses PHI to a business associate, and when the Plan requests PHI from the business associate, the Plan shall comply with the Minimum Necessary procedures herein.

When the Plan discloses PHI to a business associate, the Plan shall comply with the Accounting procedures herein. Note that under such procedures, no accounting is generally required unless the disclosure is for a purpose other than treatment, payment or health care operations.
### BUSINESS ASSOCIATE AGREEMENTS—DOCUMENT RETENTION

<table>
<thead>
<tr>
<th>Section: General</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Business Associate Agreements</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

#### POLICY

All *business associate* agreements executed by the Plan will be subject to the document retention policies set forth in these HIPAA Policies and Procedures.

#### PROCEDURE

All *business associate* agreements executed by the Plan shall be forwarded to the Privacy Officer who shall retain the documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.

The Privacy Officer or his/her designee shall monitor the return or destruction of PHI used, created or obtained by the *business associate* upon termination of the Business Associate Agreement (or the extension of protection if PHI is not returned or destroyed).
DATA USE—DE-IDENTIFIED INFORMATION

Section: General
Subsection: Data Use

Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan may disclose de-identified information without observing the other HIPAA Policies and Procedures, because de-identified information is not subject to the Rule.

Health information that does not identify an individual, that complies with this De-Identified Information Policy and Procedure and, which, in the Plan’s reasonable belief, cannot be used to identify an individual, is considered “de-identified.”

PROCEDURE

In General

Workforce Members shall not assume that information is de-identified or that information may be disclosed without regard to the protections imposed by the Rule and by these HIPAA Policies and Procedures. Workforce Members who wish to make such an unprotected disclosure shall first obtain the approval of the Privacy Officer, who shall give such approval only after confirming that the information in question has been de-identified.

Creating De-identified Information

The Plan may use PHI in order to create de-identified information, and may disclose PHI to a business associate in order to create de-identified information.

Health information may be de-identified under the supervision and subject to the documented approval of the Privacy Officer. The Privacy Officer shall approve the de-identification of health information if:

- A person with knowledge of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information disclosed could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information. The Plan must receive documentation of the methods and the result of the analysis that justify this determination; or

- The following 18 identifiers of the individual or of relatives, employers, or household members of the individual, are removed, and the Plan does not have knowledge that the information provided could be used alone or in combination with other information to identify an individual who is a subject of the information:

  (1) Names;
(2) All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip codes. The initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census:
   (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   (b) If the geographic units which make up the initial three digits of a zip code contain 20,000 or fewer people, the first three digits must be changed to 000.

(3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, 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 aggregated into a single category of age 90 or older;

(4) Telephone numbers;
(5) Fax numbers;
(6) Electronic mail addresses;
(7) Social security numbers;
(8) Medical record numbers;
(9) Health Plan beneficiary numbers;
(10) Account numbers;
(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(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, except as permitted for re-identification of the data as set forth below.

Re-identification Codes

The Privacy Officer shall approve the selection of re-identification codes for de-identified health information. Re-identification codes shall be treated in the same manner as PHI, and shall receive the protections given to PHI by the Rule and by these HIPAA Policies and Procedures.

The Plan may assign a code or other means of record identification to allow de-identified information to be re-identified, provided that:

- The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

- The Plan shall not use or disclose the code or other means of record identification for any other purpose, and shall not disclose the mechanism for re-identification.
**DATA USE—LIMITED DATA SETS**

<table>
<thead>
<tr>
<th>Section: General</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Data Use</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

The Plan may *use* a limited data set, and *disclose* it to a recipient pursuant to a Data Use Agreement, for purposes of *research*, public health or *health care operations*.

The Plan may *use PHI*, and may *disclose PHI* to a *business associate*, in order to create a limited data set.

The Plan will comply with the terms of any Data Use Agreement to which it is a party.

**PROCEDURE**

*Securing a Data Use Agreement*

A Workforce Member shall obtain a Data Use Agreement, signed by the intended recipient of a limited data set, before *disclosing* a limited data set to that recipient. Any such agreement shall:

- be approved by the Privacy Officer;
- indicate the purposes of the limited data set (*research*, public health, or specific *health care operations*);
- and specify the *uses* and *disclosures* that the recipient may make of the *PHI* in the limited data set.

The original, fully-executed Data Use Agreement should be forwarded to the Privacy Officer who shall retain the documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.

*Creating a Limited Data Set*

A limited data set shall exclude all direct identifiers of each *individual* whose *PHI* is included and of each of those *individuals’* relatives, household members, and employers. It may contain any other data, including age, any element of dates (e.g., birth dates, admission dates, discharge dates, death dates), any geographic information broader than postal addresses (e.g., municipalities, states, zip codes), and any unique identifying number, characteristic or code.

A limited data set may contain only the minimum necessary *PHI* for the purpose for which the limited data set is to be *used* or *disclosed*.

The Privacy Officer shall verify that data qualifies as a limited data set and satisfies the minimum necessary limitation before the data may be *used* or *disclosed*.
**Breach of Data Use Agreement**

The failure to comply with a Data Use Agreement may expose the Plan to sanctions.

If any Workforce Member suspects that one or more of the Plan’s Data Use Agreements has been breached, the Workforce Member shall immediately report the suspected breach to the Privacy Officer.

If the suspected breach is by the recipient of the data supplied by the Plan, the Plan shall require the recipient to promptly cure the breach. If the recipient fails to cure the breach to the Plan’s satisfaction, the Plan shall discontinue disclosing data to the other party and shall terminate the Data Use Agreement.

If the breach is by the Plan, the Privacy Officer shall conduct an investigation in the same manner as if a complaint had been filed.

If the breach involves *Unsecured PHI*, then the Privacy Officer shall follow the Plan’s HIPAA Breach Notification Policy and Procedure.

**Document Retention**

All Data Use Agreements executed by the Plan shall be forwarded to the Privacy Officer who shall retain the documents in a file specifically designed for that purpose. The files shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
VERIFICATION

Section: General
Subsection: Verification
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

Whenever these HIPAA Policies and Procedures call for the verification of someone’s identity or authority, the procedures in this Section shall be followed. The Plan does not have to recognize a personal representative for an individual if the personal representative is suspected of abusing, neglecting, or endangering the individual.

PROCEDURE

Request by an individual

Obtain appropriate evidence verifying the identity of the individual. Examples of appropriate identification include: an identification card that includes a photograph; a valid driver’s license; a government identification card or badge. If there is any question concerning such evidence, contact the Privacy Officer.

Request by a parent of a minor child

A “minor” means an individual under the age of 18 (as otherwise defined under state law) who has not been legally emancipated (given the status of an adult) by a court and is:

- Not legally or previously married;
- Not serving in the armed forces;
- Not presently an offender in the Texas Department of Criminal Justice or other correctional facility; or
- Not at least 16 years old and living away from home and managing their own financial affairs.

The Privacy Worker must obtain appropriate evidence of the parent’s identity. Examples of appropriate identification include: an identification card that includes a photograph; a valid driver’s license; a government identification card or badge. Also obtain appropriate evidence of the parent’s relationship with the child. (For example: a form confirming enrollment of the child in the parent’s Plan as a dependent or a birth certificate showing the name of both parent and child.) If there is any question concerning such evidence, contact the Privacy Officer.

Once a minor is emancipated, a guardian or parent can no longer be recognized as a personal representative.
Request by an individual’s personal representative

A “personal representative” means any adult that has decision-making capacity and who is willing to act on behalf of an individual. A personal representative would include an individual who has authority, by law, or by agreement from an individual to act in the place of the individual. This includes parents, legal guardians, or properly appointed agents, like those identified in documents like a Durable Power of Attorney, or individuals designated by state law.

The Privacy Worker must obtain appropriate evidence of the personal representative’s identity. Examples of appropriate identification include: an identification card that includes a photograph; a valid driver’s license; a government identification card or badge. Also obtain appropriate evidence of the personal representative’s authority to act for the individual. (For example: court papers appointing the personal representative; a power of attorney.) If there is any question concerning such evidence, contact the Privacy Officer.

Request by a person who purports to be a public official

Obtain appropriate evidence of the person’s identity. (For example: an agency identification badge or other official credentials.) If there is any question concerning such evidence, contact the Privacy Officer.

Request by a person who purports to be acting on behalf of a public official

Obtain appropriate evidence of the person’s identity. (See examples above.) Also obtain appropriate evidence of the person’s authority. (For example: a written statement on appropriate government letterhead that the person is acting under the government’s authority; a contract for services, memorandum of understanding, or purchase order that establishes that the person is acting on behalf of a public official.) If there is any question concerning such evidence, contact the Privacy Officer.

Request by a person acting pursuant to legal process (warrants, orders, subpoenas, and other documents) issued by a grand jury or a judicial or administrative tribunal

Do not seek verification independently. Contact the Privacy Officer immediately. If the Privacy Officer is unavailable, contact HIPAA counsel.

Request by a person who purports to be acting on behalf of a deceased individual

PHI generated during the life of an individual is protected from disclosure after death unless disclosure is for treatment, payment or health care operations. Privacy Workers cannot release PHI regarding a deceased individual unless a personal representative has been verified and the personal representative has requested the PHI through the proper authorization process.

If under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or on behalf of the individual’s estate, the Plan must recognize such person as a personal representative under these HIPAA Policies and Procedures.

Absent an executor, administrator, or other court-appointed representative for the deceased
individual’s estate, the individual’s listed below may authorize the release of PHI in order of priority. An entire category must be exhausted (i.e. no people in the category exist or are still alive) before moving to the next category. If there are questions, contact the Privacy Officer. If the Privacy Officer is unavailable, contact HIPAA counsel.

In the case of a deceased, married individual survived by a spouse with or without descendants:

- Spouse;
- Adult children;
- Adult grandchildren;
- Parents;
- Adult descendants of parents (i.e. brothers and sisters);
- Brothers’ and sisters’ adult children (i.e. nieces and nephews);
- Brothers’ and sisters’ adult grandchildren;
- Grandparents; or
- Adult descendants of grandparents (i.e. aunts and uncles).

In the case of a deceased individual with no spouse with or without descendants:

- Adult children;
- Adult grandchildren;
- Parents;
- Adult descendants of parents (i.e. brothers and sisters);
- Brothers’ and sisters’ adult children (i.e. nieces and nephews);
- Brothers’ and sisters’ adult grandchildren;
- Grandparents; or
- Adult descendants of grandparents (i.e. aunts and uncles).
DOCUMENT RETENTION

Section: General  Subsection: Document Retention  Effective Date: June 1, 2008  Last Reviewed On: September 23, 2013

POLICY

The Plan will retain a record, whether on paper or electronically, of all matters that the Rule or these HIPAA Policies and Procedures require to be documented.

PROCEDURE

The documents covered by this Document Retention Policy include all documents which are expressly subject to these HIPAA Policies and Procedures, as well as the following:

- Notice of Privacy Practices (including all revisions which become effective).
- HIPAA Policies and Procedures (including all revisions which are adopted).
- Any authorization executed pursuant to 45 CFR § 164.508.
- Any restriction to the uses or disclosures of an individual’s PHI, provided that the Plan and the individual have agreed to the restriction under 45 CFR § 164.522.
- The justification for any de-identification of PHI pursuant to 45 CFR § 164.514(b)(1).
- The designated record sets that are subject to an individual’s right of access under 45 CFR § 264.524, and the name or title of the persons or offices who are responsible for receiving and processing requests for access.
- The names or titles of the persons or offices who are responsible for receiving and processing requests for amendments under 45 CFR § 164.526.
- The information required to be included in an accounting under 45 CFR § 164.528; the written accounting that is provided to the individual; and the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.
- The name or title of the person designated as the Privacy Officer.
- The name or title of the person or office designated as the Contact Office.
- Training conducted pursuant to these HIPAA Policies and Procedures.
- Complaints concerning the Plan’s privacy practices, and the disposition of those complaints.
- Sanctions imposed pursuant to these HIPAA Policies and Procedures.
In some instances, the Plan’s *business associates* are responsible for document retention consistent with this Policy. In other instances, the documents subject to this retention policy are stored by Plan Sponsor. All questions as to the storage location of a specific document should be directed to the Privacy Officer.

All documents subject to this Policy shall be retained until 6 years after the later of (a) the date on which the document was created, or (b) the date on which the document was last effective.

The following documents shall be subject to the document retention policies set forth in these HIPAA Policies and Procedures:

- Authorization documents – authorizations, verifications of authorizations, notices concerning authorizations, and revocations – received by the Plan
- All documentation that the Plan receives or creates in conjunction with minimum necessary determinations.
- All Data Use Agreements executed by the Plan
- All *Business Associate* Agreements executed by the Plan.
- Notices of Privacy Practices.
- Privacy Protection Documents – requests for privacy protection, responses to the requests, and terminations of the privacy protection.
- Designated record sets. Also *business associates* must retain designated record sets consistent with these HIPAA Policies and Procedures.
- Titles of persons or offices responsible for receiving and processing requests for access, requests for amendments and requests for accountings by *individuals*.
- Access documents – requests for access, statements of fees for access, and notices denying access.
- Amendment documents – requests for amendment, notices granting or denying amendment, statements of disagreement, and rebuttals.
- Accounting documents – information necessary to report accountable *disclosures* upon request, all such requests that are received, all accountings that are provided in response to such requests, and any other documentation regarding the Plan’s compliance with its accounting obligations.

All documents subject to the document retention provisions set forth in these HIPAA Policies and Procedures shall be forwarded to the Privacy Officer who shall retain the documents in a file specifically designed for that purpose.
PRIVACY OFFICER

Section: Privacy
Subsection: Administrative Requirements
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan shall have a Privacy Officer, whose name and contact information will be documented in these HIPAA Policies and Procedures. The Privacy Officer is responsible for developing, maintaining, and implementing these HIPAA Policies and Procedures for the Plan related to the protection of PHI. The Privacy Officer is also responsible for overseeing the Plan’s compliance with HIPAA, the Rule, any other federal and state regulations related to participant privacy, and these HIPAA Policies and Procedures as they relate to the Rule.

PROCEDURE

Selection of Privacy Officer

The Privacy Officer is selected by the Vice President Finance & Administration, which shall review the selection as needed.

Delegation of Duties By Privacy Officer

The Privacy Officer may delegate his or her duties or responsibilities to one or more Workforce Members. However, if the duty or responsibility in question involves the use or disclosure of PHI, the duty or responsibility may be delegated only to a Privacy Worker.

Documenting the Privacy Officer

The name and contact information of the Privacy Officer are as follows:

Denise M. Covert
Associate Director, Human Resources
Trinity University
One Trinity Place
San Antonio, TX 78212
(210) 999-7507
(210) 999-7542 Fax
dcovert@trinity.edu

A written copy of this and all subsequent designations of the Privacy Officer, including the effective date of such designation(s), shall be forwarded to the Privacy Officer, who shall maintain a copy of the designation in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
**Essential Duties and Functions of the Privacy Officer**

- Provide leadership in complying with laws and regulations related to the privacy of PHI.
- Assist in the interpretation of applicable law and regulations, including the Rule.
- Address questions and complaints related to the protection of PHI, violations of these HIPAA Policies and Procedures, potential breaches of business associate agreements, and potential HIPAA Breaches.
- Monitor systems and processes for appropriate access to, use and disclosure of, and requests for PHI.
- Ensure that the authorization forms, business associate agreements, and the privacy provisions of these HIPAA Policies and Procedures conform to the requirements of the Rule.
- Ensure that the Plan’s operations and actual practice conform to the privacy provisions of these HIPAA Policies and Procedures and to the Rule.
- Audit and monitor compliance with the privacy provisions of these HIPAA Policies and Procedures and, in the event of a violation, ensure that appropriate sanctions are applied.
- Ensure that notice of HIPAA Breach is provided, where required by these HIPAA Policies and Procedures.
- Ensure that all Privacy Workers receive adequate and appropriate training concerning these HIPAA Policies and Procedures.
- Ensure that all documentation required by the Rule is maintained and retained for six (6) years from the date it was created or was last in effect, whichever is later.
- Monitor business associate agreements.
- Serve as an internal and external liaison and resource between the Plan and outside entities (including vendors, oversight agencies and other parties).
- Cooperate with the Office of Civil Rights or other oversight agencies in any investigations of privacy violations.
- Assist in fostering awareness of the importance of protecting participant privacy and developing an organizational culture committed to the protection of PHI.
## CONTACT OFFICE

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Administrative Requirements</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

The Plan will maintain an office that persons may contact in order to obtain copies of the Plan’s Notice of Privacy Practices or to submit complaints about the Plan’s privacy practices.

**PROCEDURE**

The Contact Office is selected, supervised, and directed by the Privacy Officer.

The Plan’s Contact Office is as follows:

Trinity University  
Human Resources  
One Trinity Place  
San Antonio, TX 78212-7200  
Phone: (210) 999-7507

A written copy of this and all subsequent designations of the Contact Office, including the effective date of such designation(s), shall be forwarded to the Privacy Officer, who shall maintain a copy of the designation in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
<table>
<thead>
<tr>
<th>PRIVACY WORKERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section: Privacy</td>
</tr>
<tr>
<td>Subsection: Administrative Requirements</td>
</tr>
<tr>
<td>Effective Date: June 1, 2008</td>
</tr>
<tr>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

In order for the Plan to share PHI with Privacy Workers, the Plan document shall be amended to specify such Privacy Workers. Only the Privacy Worker identified in the Plan document are permitted to access, use or disclose PHI.

**PROCEDURE**

The Plan Document has been amended to permit persons in the following positions or departments to access, use, or disclose PHI in order to perform Plan administration functions:

- President, Vice Presidents, Assistant Vice President Human Resources, Associate Director Human Resources, Employee and Benefits Administrator, Human Resources Coordinator, and Human Resources Assistant.
POLICY

The Plan shall provide training for all Privacy Workers. Privacy Workers who violate these HIPAA Policies and Procedures will be subject to the sanctions policy set forth herein and may also be subject to disciplinary action (including termination) consistent with Plan Sponsor’s policies, procedures, and business practices.

PROCEDURE

Oversight of Training

The Privacy Officer is responsible for determining which Workforce Members are Privacy Workers, which Privacy Workers should be trained, when the training should occur, and what the substance of the training should be.

Timing of Training

All new Workforce Members shall receive training before they shall be permitted to access, use, or disclose PHI.

All Privacy Workers who change positions shall receive new training (as appropriate) at the time of the change.

All Privacy Workers shall receive retraining periodically or upon a material change in these HIPAA Policies and Procedures.

Documenting of Training

All training shall be documented.

The documentation shall be completed by the trainer and shall include, at a minimum: the name of the Privacy Worker trained; the date of the training; the name of the individual providing the training; and a summary of the substance of the training.

The documentation shall be forwarded to the Privacy Officer, who shall maintain a copy of all such documentation in a single file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
FORM: OCCURRENCE OF HIPAA PRIVACY TRAINING

HIPAA PRIVACY TRAINING

Name of Trainer: ____________________________________________________________

Date of Training: ___________________________________________________________

Individuals Attending Training: (if the space provided is insufficient, attach additional sheets)
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________

Summary of Training: (if the space provided is insufficient, attach additional sheets)
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________

____________________________
Date

____________________________
Signature
ACKNOWLEDGEMENT OF HIPAA PRIVACY TRAINING

I acknowledge that I have attended the HIPAA Training held on __________________________ (MM/DD/YYYY), in its entirety.

I agree to abide by the HIPAA Policies and Procedures adopted by the Plan so that the Plan may comply with HIPAA and its regulations.

I acknowledge that my failure to comply with these HIPAA Policies and Procedures may subject me to sanctions including, but not limited to, written reprimands, suspension or termination of my employment.

______________________________
Date

______________________________
Signature

______________________________
Print Name
COMPLAINTS

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Administrative Requirements</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

POLICY

The Plan will timely investigate and appropriately respond to each written complaint received by the Contact Office which concerns compliance (or the failure to comply) with the Rule and/or these HIPAA Policies and Procedures.

PROCEDURE

All complainants should be directed to the Contact Office so that the appropriate procedures can be followed. Complaint forms are available from the Contact Office.

The complainant shall submit a written complaint. The complainant is not required to use an official complaint form, but should be encouraged to do so. If the complainant wishes to submit a complaint to the Office for Civil Rights (OCR), the complaint form is publicly available at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintpackage.pdf. The Secretary or OCR may investigate complaints filed under these HIPAA Policies and Procedures. Such investigation may include a review of pertinent policies, procedures, or practices of the Plan and of the circumstances regarding any alleged acts or omissions concerning compliance.

**Processing a Complaint**

When a Workforce Member at the Contact Office first receives a complaint, the Workforce Member shall not indicate to the complainant what the Plan or Plan Sponsor shall do in response to the complaint. In addition, the Workforce Member shall take each of the following steps:

- Confirm that the complainant’s name and address are on the complaint and are legible.
- As near to the top of the complaint as possible, print the date and time when the complaint was received, the name of the Workforce Member initially receiving the written complaint, and (if there is more than one contact office) the location of the office where the complaint was received.
- Forward the original complaint to the Privacy Officer.

The Privacy Officer shall be responsible for investigating all complaints and for documenting the investigation. Workforce Members shall fully and timely cooperate with any such investigation. The Privacy Officer shall document the course of the investigation, as well as the Privacy Officer’s findings and conclusions.

After the Privacy Officer has completed the investigation, made findings, and reached a conclusion, the Privacy Officer shall prepare a written response to the complainant. The
response shall be sent via regular U.S. mail to the complainant at the complainant’s home address.

The response shall indicate in general terms the course of the investigation, findings and conclusions, and the corrective action, if any, that shall be taken. The Privacy Officer is not required to advise the complainant of the persons involved in the investigation. Likewise, if the corrective action includes sanctions or discipline imposed upon a Workforce Member, the Privacy Officer is not required to provide the complainant with details of the corrective action.

If the Privacy Officer concludes that corrective action is warranted, the Privacy Officer shall take appropriate steps in order to correct the matters complained of. The Privacy Officer shall document these steps, confirming in writing that the corrective action was completed or implemented.

**Documenting the Complaint**

The following documentation concerning a Complaint shall be forwarded to the Privacy Officer:

- The original complaint, including information concerning the receipt of the complaint.
- The course of the investigation, findings, and conclusions by the Privacy Officer.
- The corrective action, if any, taken following the investigation.
- The response sent to the complainant.

The Privacy Officer shall maintain a copy of all such documentation in a single file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
SANCTIONS

Section: Privacy
Subsection: Administrative Requirements
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan shall apply sanctions against any Workforce Member who violates these HIPAA Policies and Procedures.

PROCEDURE

- In conjunction with Plan Sponsor’s Human Resources Department, the Privacy Officer may, but is not required to, develop written guidelines and/or procedures for imposing sanctions for violations of these Policies and Procedures. When developed, these written guidelines and procedures shall be appended to these HIPAA Policies and Procedures and shall be distributed to all Privacy Workers.

- Until such time as the Privacy Officer develops guidelines and/or procedures for addressing violations of these HIPAA Policies and Procedures, the sanctions for such violations shall be determined and imposed through the ordinary disciplinary process established by Plan Sponsor, except as set forth in the remainder of this paragraph. For any violation of these HIPAA Policies and Procedures, to the extent that the ordinary disciplinary process does not already include the Privacy Officer, the Privacy Officer shall become an integral part of such process. If the ordinary disciplinary process calls for the final determination on discipline to be made by a Workforce Member (such as the Human Resources Director), the final determination on discipline for a violation of these HIPAA Policies and Procedures shall be made by or in consultation with the Privacy Officer.

- Sanctions shall be applied against any Workforce Member who violates these HIPAA Policies and Procedures. The sanction shall be determined based on the nature of the violation, its severity, and whether it was intentional or unintentional. Sanctions may include verbal warnings, written warnings, probationary periods with or without pay, alteration in duties / job reassignment or termination.

- In the event that sanctions are imposed, the Privacy Officer shall write a report, which shall include, at a minimum: the name of the Workforce Member; the nature of the privacy violation; and the sanction imposed. The report shall be forwarded to the Privacy Officer, who shall maintain a copy of the report in a file specifically designated for such reports. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.

- Sanctions shall not be applied against Workforce Members who file a complaint concerning a violation of these HIPAA Policies and Procedures or of the Rule. Sanctions shall not be applied against Workforce Members who refuse to follow a policy or procedure that they
believe, in good faith, violates the Rule.
| Current Date:  |  |
| Date of Incident:  |  |
| Name of Complainant:  |  |
| Name of Employee alleged to have violated the HIPAA Policies and Procedures:  |  |
| Described the process of investigating the Complaint:  |  |
| Describe the corrective measured taken, if any (include the date on which such measures were taken):  |  |
| Name of Privacy Officer:  |  |
| Signature of Privacy Officer:  |  |
| Date Signed:  |  |
## MITIGATION

<table>
<thead>
<tr>
<th>Section: Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Administrative Requirements</td>
</tr>
<tr>
<td>Effective Date: June 1, 2008</td>
</tr>
<tr>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

### POLICY

To the extent practicable, the Plan shall mitigate any known harmful effects of an improper use or disclosure of PHI by a Workforce Member or by a business associate.

### PROCEDURE

The Privacy Officer will consider mitigation as part of any investigation concerning an improper use or disclosure of PHI.

The Plan will take reasonable steps based on the nature of the improper use or disclosure, how the use or disclosure might cause harm to an individual, and what steps might mitigate that harm.

Workforce Members shall fully cooperate in such mitigation efforts. Mitigation efforts may include, but are not limited to, the following:

- Taking operational and procedural corrective measures to remedy violations;
- Taking employment actions to re-train, reprimand, or discipline Workforce Members pursuant to the Sanctions Policy;
- Addressing problems and issues with business associates;
- Incorporating mitigation solutions into these HIPAA Policies and Procedures as appropriate.

Any mitigation steps taken shall be included in the Privacy Officer’s report concerning the investigation.
## NO RETALIATION OR INTIMIDATION

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Administrative Requirements</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

### POLICY

The Plan and Plan Sponsor will not retaliate against any person who files a HIPAA complaint.

The Plan and Plan Sponsor will not intimidate any person who files a HIPAA complaint.

### PROCEDURE

No Workforce Member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any person:

- For exercising his or her rights under HIPAA or for filing a complaint or participating in other processes established by these HIPAA Policies and Procedures;
- For testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing involving a HIPAA complaint; or
- For opposing any act or practice made unlawful by HIPAA, provided the individual or person or entity has a good faith belief that the practice opposed is unlawful. The manner of the opposition must be reasonable and must not involve an improper disclosure of PHI. For example, an employee who discloses PHI to the media or friends is not protected by this Policy.

Any Workforce Member who suspects that there has been a violation of this Policy shall report the suspicion to the Privacy Officer. Such a report may be made anonymously.

All Workforce Members shall cooperate fully with any investigation, corrective action, or sanction instituted by the Privacy Officer.
NO WAIVER OF RIGHTS

Policy:

No individual will be required to waive any right under HIPAA, including the right to complain to the Secretary, as a condition of the Plan providing claims payment, enrollment, or benefits eligibility to the individual.

Procedure:

Any Workforce Member who suspects that there has been a violation of this policy shall report the suspicion to the Privacy Officer. Such a report may be made anonymously.

All Workforce Members shall cooperate fully with any investigation, corrective action, or sanction instituted by the Privacy Officer.
AUTHORIZATIONS—CORE POLICIES

Section: Privacy
Subsection: Authorizations

Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

Whenever the Plan uses or discloses PHI, except for those uses or disclosures expressly permitted by these HIPAA Policies and Procedures, the Plan will first obtain a completed and HIPAA-compliant authorization. The Plan shall adhere strictly to the details of the authorization, and shall not act or rely on an authorization that, to the Plan's knowledge, has expired or has been revoked.

The Plan shall not require any individual to complete an authorization as a condition of payment, enrollment, or eligibility for benefits.

Signing the authorization form is voluntary and the individual may refuse to sign it.

When the Plan is presented with a valid authorization for a use or disclosure of an individual’s PHI, the Plan is permitted, but not required, to make such use or disclosure.

The Plan will not seek authorizations for marketing communications or for fundraising.

PROCEDURE

If a Workforce Member has any question as to whether an authorization is necessary or appropriate, he or she shall contact the Privacy Officer to determine whether an authorization form should be used.
### POLICY

An authorization to *use* or *disclose* psychotherapy notes may not be combined with any other authorization.

### PROCEDURE

When the Plan seeks an authorization to *use* or *disclose* psychotherapy notes, it shall not use the same authorization to seek the *use* or *disclosure* of any other PHI. When the Plan receives an authorization seeking the *disclosure* of psychotherapy notes, the Plan shall not *disclose* such notes unless the Plan first confirms that the authorization does not seek the *disclosure* of any other PHI.
# AUTHORIZATIONS—REQUESTED BY A PARTICIPANT OR BY THE PLAN

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date:</th>
<th>Last Reviewed On:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Authorizations</td>
<td>June 1, 2008</td>
<td>September 23, 2013</td>
</tr>
</tbody>
</table>

## POLICY

To the extent possible, the Plan will use a standardized authorization form. The Plan's authorization form will contain all of the elements required by the Rule.

## PROCEDURE

**Standardizing Authorization Forms**

An updated copy of the standardized authorization form can be obtained from the Privacy Officer or the Contact Office. When a Plan participant requests an authorization form from any Workforce Member, the Workforce Member shall either provide the standardized form, or shall direct the *individual* to the Privacy Officer or the Contact Office.

**Completing An Authorization**

Whenever an authorization is sought by an *individual*, a Privacy Worker, or a Workforce Member, each of the steps set forth below shall be followed:

- Fill in the authorization form, or have it filled in by the *individual* or the *individual's* personal representative.

- Have the *individual*, or the *individual's* personal representative, read, sign, and date the authorization. If the authorization is signed by the *individual's* personal representative, be sure that the authorization indicates the nature of the personal representative's relationship to the *individual*.

- Verify the identity of the *individual*, or of the *individual's* personal representative as set forth in the Verification Policy.

- Give the *individual*, or the *individual's* personal representative, a copy of the signed authorization.

- Forward the original authorization to the Privacy Officer, who shall be responsible for document retention. The Privacy Officer will also be responsible for directing the authorized use or disclosure.
Defective Authorizations

- An authorization is invalid if it is incomplete. An authorization is also invalid if it contains information that is known to be false by the individual completing the form, or by the Workforce Member reviewing the form.

- An authorization for the use or disclosure of psychotherapy notes may not also authorize the use or disclosure of other types of PHI.

- The expiration of the authorization has passed or the expiration event is known to have occurred.

- The authorization is known to have been revoked.

- The authorization lacks any one of the core elements described in the Checklist for Validating Authorizations.
## AUTHORIZATIONS—RECEIVED FROM ANOTHER

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Authorizations</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

### POLICY

When the Plan is presented with a valid authorization for a *use* or *disclosure* of an individual's PHI, the Plan is permitted, but not required, to make such *use* or *disclosure*.

### PROCEDURE

Upon receiving a document which claims to be an authorization allowing the Plan to *use* or *disclose* PHI, the person receiving the document shall:

- Verify the identity of the *individual*, or of the *individual’s* personal representative as set forth in the Verification Policy.
- Forward the original authorization to the Privacy Officer, who shall be responsible for document retention.
- The Privacy Officer shall be responsible for directing the authorized *use* or *disclosure*. 
# AUTHORIZATIONS—REVOCATION

<table>
<thead>
<tr>
<th><strong>Section:</strong> Privacy</th>
<th><strong>Effective Date:</strong> June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subsection:</strong> Authorizations</td>
<td><strong>Last Reviewed On:</strong> September 23, 2013</td>
</tr>
</tbody>
</table>

## POLICY

The Plan is not permitted to rely upon an authorization that the Plan knows to be revoked. An authorization may be revoked at any time. Revocation of an authorization does not affect any actions that the Plan took before the Plan learned of the revocation.

## PROCEDURE

The Plan does not have a standard form for revoking an authorization. If an *individual*, or an *individual's* personal representative, who has given the Plan an authorization indicates a desire to revoke the authorization, the revocation shall be documented as follows:

- The revocation shall be in writing and shall provide enough information about the authorization being revoked, so that given the facts and circumstances, the authorization being revoked can be accurately identified. In most instances, it shall be sufficient to include the name of the *individual* and the date of the authorization; in some cases (for example, when an *individual* has executed multiple authorizations), additional detail may be necessary.

- Have the *individual*, or the *individual's* personal representative, sign and date the revocation. If the authorization is signed by the *individual's* personal representative, be sure that the revocation indicates the nature of the personal representative's relationship to the *individual*.

- Verify the identity of the *individual*, or of the *individual's* personal representative, as set forth in the Verification Policy.

- Give the *individual*, or the *individual's* personal representative, a copy of the signed revocation.

- Forward the original revocation to the Privacy Officer, who shall be responsible for document retention.
AUTHORIZATIONS—USING OR DISCLOSING PHI ACCORDINGLY

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Authorizations</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

Any *use or disclosure* pursuant to an authorization shall be approved by the Privacy Officer.

Any *disclosure* pursuant to an authorization does not need to be included on the Plan’s accounting log.

Any *use or disclosure* pursuant to an authorization does not need to be the minimum necessary to accomplish the purpose of the *use or disclosure*, but the terms of the authorization shall be strictly followed.

**PROCEDURE**

Upon receipt of an authorization directing the *use or disclosure* of an individual’s PHI, the Privacy Officer shall take the following steps:

- If the authorization is not the Plan’s form authorization, the Privacy Officer shall confirm that the authorization contains all of the information necessary to be HIPAA-compliant as set forth in the Checklist for Validating Authorizations. If the Privacy Officer determines that the Authorization is not valid, the Privacy Officer shall send a written notice to the individual indicating the deficiency. The Privacy Officer shall retain a copy of the written notice for documentation purposes, and shall not take the remaining steps in this procedure.

- The Privacy Officer shall confirm that the authorization has not expired or been revoked.

- If verification has not already occurred, the Privacy Officer shall verify the identity of the *individual* and/or the *individual’s* personal representative as set forth in the Verification Policy.

- The Privacy Officer shall determine whether the *disclosure* should be made.

- If the Privacy Officer determines that the *disclosure* should not be made, the Privacy Officer shall notify the *individual* of this determination in writing. The Privacy Officer shall retain a copy of the notice for documentation purposes.

- If the Privacy Officer determines that the *disclosure* should be made, the Privacy Officer shall take, or direct others to take, the necessary steps to make the *disclosure*. 
## AUTHORIZATIONS—DOCUMENT RETENTION

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Authorizations</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

### POLICY

The authorization documents—authorizations, verifications of authorizations, notices concerning authorizations, and revocations—received by the Plan will be subject to the document retention policies set forth in these HIPAA Policies and Procedures.

### PROCEDURE

The Privacy Officer shall maintain a copy of the authorization documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
FORM: AUTHORIZATION

[A separate authorization must be used if the authorization is for psychotherapy notes.]

Name: ________________________________          Birth Date: ___/___/___
Address: __________________________________________
Telephone: ___________________________          Soc. Sec. # __________________________
E-mail: __________________________________________

By signing this authorization form I authorize the person(s) and/or organization(s) described below to use and/or disclose my health information (information that constitutes protected health information as defined in the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996) in the manner described below. I understand that I am under no obligation to sign this form. The person(s) and/or organization(s) described below who I am authorizing to use and/or disclose my information may not condition treatment, payment, enrollment in a health plan or eligibility for health care benefits on my decision to sign this authorization, except as follows:

I have signed this form voluntarily to document my wishes regarding the use and/or disclosure of the health information described below in Section 1 of this form.

1. Description of Health Information I Authorize to be Used or Disclosed. The following is a specific description of the health information I authorize be used and/or disclosed: (Specify and provide a meaningful description.)

2. Persons/Organizations Authorized to Use and/or Disclose My Health Information. I authorize the following person(s) and/or organization(s) (or classes of persons and/or organizations), including the Trinity University Group Health Plan (the “Plan”), to use and/or disclose the health information described above in Section 1 of this form.

3. Persons/Organizations authorized to receive and/or use my health information. I authorize the following person(s) and/or organization(s) (or classes of persons and/or
organizations) to receive my health information from the person(s) and/or organization(s) described in section 2 above and to use or disclose such information for the purposes listed below in section 4 of this form. I understand that if neither federal or Texas privacy law apply and the person(s) and/or organization(s) listed below are not health care providers, health plans or health care clearinghouses subject to federal privacy standards, the health information disclosed pursuant to this authorization may no longer be protected by the federal privacy standards and such person(s) and/or organization(s) may re-disclose my health information without obtaining my authorization.

4. Description of Each Purpose for the Requested Use and/or Disclosure. I authorize my health information to be used and/or disclosed for the following specific purposes:

5. Rights with Respect to This Authorization.
   5.1 Right to Revoke. I understand that I have the right to revoke this authorization at any time by notifying the Plan in writing at the following address: Trinity University, Attn: Privacy Officer, One Trinity Place, San Antonio, TX 78212-7200. I also understand that my revocation of this authorization must be in writing. I am aware that my revocation will not be effective as to uses and/or disclosures of my health information that the person(s) and/or organization(s) identified in Sections 2 and 3 of this form have already made in reliance upon this authorization.

   5.2 Right to Inspect or Copy the Health Information to be Used or Disclosed. I understand that I have the right to inspect or copy the health information I have authorized to be used or disclosed in accordance with this form. I may arrange to inspect my health information or obtain copies of my health information by contacting [insert title of contact person, address and telephone number].

   5.3 Right to Receive Copy of This Authorization. I understand that if I agree to sign this authorization, which I am not required to do, I must be provided with a signed copy of it.

6. This authorization will expire (choose and complete one):

   ☐ On _______/______/______.

   ☐ Upon the occurrence of the following event(s) related to my health care or to the purpose(s) for which I have authorized the use and/or disclosure of my health information described in
Section 3 of this form:
__________________________________________________________
__________________________________________________________
__________________________________________________________

I, _________________________________________________ (please print name), have had an opportunity to review and understand the contents of this form. By signing this form, I am confirming that it accurately reflects my wishes.

__________________________________________________________  ____/____/____
Signature                                                     Date

If signed by a personal representative, complete the following:

Name of personal representative: ________________________________

Relationship to participant or nature of authority (e.g., health care power of attorney, guardian, other statutory authorization): ________________________________

Address: ______________________________________________________
__________________________________________________________
__________________________________________________________

Home Telephone Number: ___________ E-mail: ______________________
Work Telephone Number: ______________

__________________________________________________________  ____/____/____
Signature of Personal Representative                        Date
# CHECKLIST: VALIDATING AUTHORIZATIONS

To be valid, an authorization must contain each of the following:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- The name or other specific identification of the person(s), or class of persons, to whom the Plan may make the requested use or disclosure.

## Core Elements of a Valid Authorization

A valid authorization must contain at least the following elements and must be written in plain language:

- A description of the PHI to be used or disclosed that identifies the PHI in a specific and meaningful fashion.
- The name or other specific identification of the person or class of persons authorized to make the requested use or disclosure.
- The name or other specific information of the person or class of persons to whom the Plan may make the requested use or disclosure.
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. (The statement “end of research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository.) However, under Texas law, which is more restrictive than HIPAA, an authorization is valid until the 180th day after the date the authorization is signed, unless the authorization provides otherwise or unless the authorization is revoked.
- A description of each purpose of the requested use or disclosure. (The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.) Requests from Community Based Clinics, Texas Department of Criminal Justice, Regional Maternal Child Health Program Clinics, and requests for substance abuse records, including Employee Assistance Program records, must state the purpose of the request.
- Signature of the individual or individual’s personal representative. If the authorization is signed by a personal representative of the individual, a description of such personal representative’s authority to act for the individual shall also be provided.
- Date.
In addition to the above elements, the authorization must contain statements adequate to place the *individual* on notice of all of the following:

- The *individual's* right to revoke the authorization in writing, and any exceptions to that right.
- The *individual's* right to inspect or receive a copy of the *PHI* disclosed.
- The *individual's* right to refuse to sign the authorization.
- The ability or inability to condition *treatment*, *payment*, enrollment or eligibility for benefits on the authorization.
- The potential for information *disclosed* pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by HIPAA.
- If the *use* or *disclosure* will result in direct or indirect remuneration to the Plan from a third party, the authorization must include a statement that such remuneration will be received by the Plan.
MINIMUM NECESSARY—CORE POLICIES

Section: Privacy
Subsection: Minimum Necessary

Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan will make reasonable efforts to access, use, disclose, and request of another covered entity only the minimum PHI necessary to accomplish the Plan’s intended purpose.

This Minimum Necessary Policy does not apply to any of the following:

- **Disclosing PHI** to a health care provider for treatment purposes.
- Requesting PHI from a health care provider for treatment purposes.
- **Disclosing PHI** to an individual or the individual’s personal representative.
- **Using or disclosing PHI** pursuant to an authorization.
- **Disclosing PHI** to the Secretary for complaint investigation, compliance review, or compliance enforcement.
- **Using or disclosing PHI** as required by law.
- **Using or disclosing PHI** as required by HIPAA and the Rule.

PROCEDURE

Privacy Workers shall access, use, and disclose that PHI which is necessary to perform their duties. Privacy Workers shall not attempt to access, use, or disclose more than the minimum necessary PHI. Questions concerning the Minimum Necessary Policy, and its application to Privacy Workers, should be directed to the Privacy Officer.

*Initial Implementation*

The Privacy Officer shall identify and document the categories of PHI that each Privacy Worker needs in order to perform his or her duties, as well as any limitations or conditions appropriate to each Privacy Worker’s access to, use of, or disclosure of PHI.

The Privacy Officer shall circulate this information to the Privacy Workers.
MINIMUM NECESSARY—USES AND DISCLOSURES OF PHI

Section: Privacy
Subsection: Minimum Necessary
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan uses and discloses the minimum amount of PHI necessary to achieve the purpose of the use or disclosure.

With respect to routine or recurring uses or disclosures of PHI that are subject to the Minimum Necessary Core Policy, the Plan will follow standard protocols for determining the minimum necessary PHI.

With respect to non-routine or non-recurring uses or disclosures of PHI that are subject to the Minimum Necessary Core Policy, the Privacy Officer will determine the minimum necessary PHI to request.

PROCEDURE

Routine or Recurring Uses and Disclosures

The Privacy Officer shall identify and document each of the following:

- The Plan's routine or recurring uses or disclosures of PHI.
- The categories of PHI needed to accomplish the purpose of each routine or recurring use or disclosure.
- Any conditions appropriate to each routine or recurring use or disclosure for those categories of PHI.

Based on the above information, the Privacy Officer shall develop and issue standard protocols stating the minimum necessary PHI for each of the routine or recurring uses or disclosures. The Privacy Officer shall distribute these protocols to each Privacy Worker, who shall be responsible for following the protocols.

Non-Routine and Non-Recurring Disclosures

If a Privacy Worker believes a use or disclosure is needed to perform a Plan administration function but the use or disclosure is not covered by an existing protocol, the Privacy Worker shall contact the Privacy Officer. The Privacy Officer shall be responsible for determining what PHI is the minimum necessary for such use or disclosure.
### MINIMUM NECESSARY—REQUESTING PHI

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Minimum Necessary</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

#### POLICY

The Plan shall request the minimum amount of PHI necessary to achieve the purpose for which the PHI is being requested from a covered entity or a business associate.

With respect to routine or recurring requests that are subject to the Minimum Necessary Core Policy, the Plan will follow standard protocols for determining the minimum necessary PHI to request.

With respect to non-routine or non-recurring requests that are subject to the Minimum Necessary Core Policy, the Privacy Officer will determine the minimum necessary PHI to request.

#### PROCEDURE

**Routine or Recurring Requests**

The Privacy Officer shall identify and document each of the following:

- The Plan's routine or recurring requests for PHI from covered entities or business associates.
- The categories of PHI needed to accomplish the purpose of such requests.
- Any conditions appropriate to each such requests.

Based on the above information, the Privacy Officer shall develop and issue standard protocols stating the minimum necessary PHI for each of the routine or recurring requests. The Privacy Officer shall distribute these protocols to each Privacy Worker, who shall be responsible for following the protocols.

**Non-Routine and Non-Recurring Disclosures**

If a Privacy Worker believes that PHI should be requested from a covered entity or business associate but that the request is not covered by an existing protocol, the Privacy Worker shall contact the Privacy Officer. The Privacy Officer shall be responsible for determining what PHI is the minimum necessary for such request.
**MINIMUM NECESSARY—RESPONDING TO A REQUEST FOR PHI**

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Minimum Necessary</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

In response to a request for PHI, if the disclosure is permitted or required by the Rule and by these HIPAA Policies and Procedures, the Plan shall disclose the minimum amount of PHI necessary to achieve the purpose of the request.

**PROCEDURE**

*Requests to Disclose Entire Record*

The Plan shall not disclose a participant’s entire record for any purpose unless a justification for such a disclosure is documented.

*Routine and Recurring Requests*

The Privacy Officer shall identify and document each of the following:

- The routine or recurring requests for PHI that the Plan receives.
- The categories of PHI needed to accomplish the purpose of such requests.
- Any conditions appropriate to each such requests.

Based on the above information, the Privacy Officer shall develop and issue standard protocols stating the minimum necessary PHI for each of the routine or recurring requests. The Privacy Officer shall distribute these protocols to each Privacy Worker, who shall be responsible for following the protocols.

*Other Requests*

If a Privacy Worker believes that PHI should be requested from a covered entity or business associate but that the request is not covered by an existing protocol, the Privacy Worker shall contact the Privacy Officer. The Privacy Officer shall be responsible for determining what PHI is the minimum necessary for such request.

*Reliance*

The Plan may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when the information is requested by any of the following:
• A covered entity.

• A professional (such as an accountant or an attorney) who is either a Privacy Worker or a business associate, and who represents that the minimum necessary is being requested.

• A government agent or law enforcement official who represents that the minimum necessary is being requested.

• A researcher who represents or provides appropriate documentation that the minimum necessary is being requested.

If a Privacy Worker relies upon a request for disclosure of PHI as being a request for the minimum necessary PHI, the Privacy Worker shall take all of the following steps:

• Document the details of the request, including the name of the Privacy Worker, the date of the request, the name of the individual and/or entity making the request, and the PHI requested.

• Verify that the requester is a covered entity, professional, government agent, or researcher.

• Document the verification.

• Forward the documentation of the request and the verification to Privacy Officer, who shall retain the documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
**MINIMUM NECESSARY—DOCUMENT RETENTION**

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Minimum Necessary</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

All documentation that the Plan receives or creates in conjunction with minimum necessary determinations shall be subject to the document retention policies set forth in these HIPAA Policies and Procedures.

**PROCEDURE**

All documentation that the Plan receives or creates in conjunction with minimum necessary determinations shall be forwarded to the Privacy Officer who shall retain the documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
RIGHT TO NOTICE OF PRIVACY PRACTICES

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
</table>

**POLICY**

The Plan shall create, distribute, and maintain a written Notice of Privacy Practices (“Notice”) which shall serve to inform individuals of the ways in which the Plan may use and disclose the individual’s PHI. The Plan shall only use and disclose PHI in the ways explained in the Notice.

**PROCEDURE**

*Content of Notice*

The Plan will develop a Notice which conforms to the content requirements of the Rule, and in particular, with the requirements of 45 CFR § 164.520(b).

The Notice will describe the potential uses and disclosures of PHI by the Plan as well as an individual’s rights with respect to PHI. The Notice will include a provision reserving the Plan’s right to revise the Notice and to make the revisions applicable to all PHI that the Plan creates or maintains. The Notice will include a provision explaining how revised Notices will be distributed.

Before a Notice can become effective, it shall be approved by the Privacy Officer. Each Notice shall indicate the date on which it becomes effective.

Any use or disclosure of PHI by the Plan shall be made in a manner which is consistent with the Notice.

*Distribution of Notice*

To the extent the Plan offers a benefit through a health insurance issuer, the health insurance issuer has the legal responsibility to distribute the Notice to the appropriate individuals. Likewise, the health insurance issuer bears the legal responsibility to create policies and procedures that protect and ensure the individual’s right to a Notice.

To the extent the Plan offers a benefit which is self-insured, the drafting and distributing of the Notice is the legal responsibility of the Plan and will be governed by these HIPAA Policies and Procedures.

The Notice shall be provided to the Plan participant who is an employee or former employee. The Plan will not separately distribute a Notice to the participant’s spouse or dependents, unless the spouse or dependent has individually elected COBRA continuation coverage.
The Notice is available to anyone who requests it. Participants have the right to receive a paper copy of the Notice, even if they previously agreed to receive the Notice electronically.

The timing of the distribution shall be as follows:

- The Notice shall be distributed to all new participants upon enrollment in the Plan.
- A revised Notice shall be distributed within 60 days of any material revision to the Notice, unless the revised Notice is posted on the Plan’s website as described below.
- Participants shall be notified at least once every 3 years of the availability of the Notice and provided with instructions on how to obtain it.

Distribution of the Notice will be made through one of the following methods:

- The Notice may be distributed in person, through interoffice mail, through the U.S. Mail or electronically as described below.
- If the Plan maintains a web site that provides information about the Plan’s benefits or customer services, then the Privacy Officer will ensure that the Notice is prominently posted and available on the web site.
- The Notice may be distributed to *individuals* by e-mail, if the *individual* agrees to electronic notice and such agreement has not been withdrawn. If the Plan knows that the e-mail transmission has failed, a paper copy of the Notice will be provided to the *individual*.
- An *individual* who is the recipient of an electronic copy of the Notice shall retain the right to obtain a paper copy of the Notice from the Plan upon request.

**Notice Revisions**

The Notice is revised as needed to reflect any material changes in the Plan’s privacy practices, the Plan’s legal duties, the *individuals’* rights, or these HIPAA Policies and Procedures. Revisions to the policies and procedures are not implemented prior to the effective date of the revised Notice.

In the event the Plan makes a material change to a privacy practice included in the Notice, the Plan shall make the material changes available as follows:

- If the Plan posts its Notice on its website, the Plan must prominently post the material changes or the revised Notice on its website by the effective date of the material change(s) to the Notice. The Plan must also provide the revised Notice or information about the material changes and how to obtain the revised Notice, in its next annual mailing to individuals then covered by the Plan (e.g. during open enrollment).
- If the Plan does not post its Notice on a website, the Plan must provide the revised Notice or information about the material change and how to obtain the revised Notice, to individuals.
then covered under the Plan within 60 days of the material revision to the Notice.

**Document Retention**

The Privacy Officer shall maintain a copy of each Notice in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
RIGHT TO REQUEST RESTRICTIONS

Section: Privacy
Subsection: Individual Rights
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

*Individuals* have the right to request that the Plan restrict how their *PHI* is *used or disclosed* for *treatment, payment* and *health care operations*, and how their *PHI* is *disclosed* to specified persons. If the Plan agrees to such a request, it will comply with the agreed-upon restriction, and advise its Privacy Workers and *business associates* to do likewise, until the restriction is properly terminated.

The Plan has no obligation to agree to such a request, unless: (i) the *disclosure* is to a health plan for purposes of *payment* or *health care operations*; or (ii) the *PHI* pertains solely to a health care item or service for which the health care provider involved has been paid in full by the *individual*.

PROCEDURE

*Requesting a Restriction*

An *individual’s* request for a restriction must be in writing. The request shall include: the *individual’s* name and contact information; the *PHI* to which the restriction applies; the requested restriction; the dates on which the restriction is requested to begin and end; the date of the request; and the *individual’s* signature.

If the request is first received by a Workforce Member, the Workforce Member shall verify the identity of the *individual*, write the date and time of receipt on the top of the first page of the request, and forward the request to the Privacy Officer. The Workforce Member shall not tell the *individual* whether the Plan shall agree to the restriction.

*Processing a Request for Restriction*

A request for a restriction shall be forwarded to the Privacy Officer. The Privacy Officer has the sole authority to grant or deny requests for restrictions.

The Privacy Officer shall respond to all requests for restriction in writing, within the time frames set forth in this Policy.

Within 30 days of receiving a request for a restriction, the Privacy Officer shall make a determination as to whether to accept the restriction.

The Privacy Officer must grant the request if:

- the *disclosure* is to a health plan for purposes of carrying out *payment* or *health care* operations.
operations (and is not for purposes of carrying out treatment); and

- the PHI pertains solely to a health care item or service for which the health care provider has been paid in full by the individual.

Except as described immediately above, the Privacy Officer shall not agree to any restriction that is, in the sole judgment of the Privacy Officer, unenforceable. For purposes of this procedure, a restriction is unenforceable if it prevents the use or disclosure of PHI for purposes of carrying out treatment, permitted public interest or benefit activities, or prevents disclosure to the Secretary for compliance investigation or enforcement.

The Privacy Officer shall respond to the individual in writing, advising the individual of the determination. The individual shall be informed that despite the restriction, the Plan may disclose the individual’s PHI to a health care provider if needed for emergency medical treatment.

**When a Request for Restriction Is Granted**

When the Plan agrees to a request for restriction, the Privacy Officer shall notify the affected Privacy Workers and business associates, in writing, of such restrictions.

A notation will be made in the individual’s record(s).

The Plan will not use or disclose PHI inconsistent with the restriction.

Although a request for restriction has been granted, the Plan may disclose the PHI, if requested to do so, for emergency medical treatment of the individual. In the event of a such a request, the applicable procedures are as follows:

- Any request for the Plan to disclose restricted PHI for treatment of an individual in a medical emergency shall be immediately forwarded to the Privacy Officer for determination. If the Privacy Officer is unavailable to make this determination, then [insert title of appropriate person] may stand in for the Privacy Officer.

- The Privacy Officer (or the stand-in) shall exercise professional judgment to determine whether the medical emergency justifies using or disclosing the restricted PHI and shall document the basis for the determination, regardless of the outcome of the determination.

**When a Request for Restriction Is Denied**

The individual will be given the opportunity to discuss his or her privacy concerns, if desired. Efforts will be made to assist the individual in modifying the request for restrictions to accommodate his or her concerns and obtain acceptance by the Plan.

**Termination of Restriction**

Unless granting the restriction was mandatory, the Plan may terminate a restriction with or
without the agreement of the individual.

Only the Privacy Officer may terminate a restriction on behalf of the Plan. To terminate a restriction, the Privacy Officer shall take all of the following steps:

- Notify the individual, in writing, that the Plan is terminating the restriction, and request that the individual concur in the termination, either verbally or in writing. If the individual verbally agrees to termination of the restriction, the Plan will document the individual’s agreement. If the individual does not concur with the termination, any PHI that was created or received prior to the termination notice will remain subject to the restriction.

- Notify the affected Privacy Workers and business associates that the restriction has terminated and, if applicable, that restriction shall continue to apply to PHI that was created or received subject to the restriction.

**Document Retention**

The Privacy Officer shall maintain a copy of the determination and any related documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
FORM: REQUEST FOR RESTRICTIONS

Name: ___________________________________________ Birth Date: ____/____/____
Address: ____________________________________________________________
Telephone: ___________________________ Soc. Sec. # _______________________
E-mail: ______________________________________________________________

I hereby request a restriction on the way in which the Trinity University Group Health Plan
and/or the Trinity University Flexible Benefit Plan (the “Plan”) uses and discloses my health
information (information protected by HIPAA). I understand that except in limited
circumstances, the Plan may deny this request. I also understand that even if this request is
granted, the Plan will generally be allowed to disclose my PHI for purposes of emergency
medical treatment. I understand that even if the Plan grants my request, the Plan may remove
this restriction in the future, if I am notified in advance.

The following is a description of the specific health information I would like to restrict and the
way in which I would like to have it restricted:

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

By signing this form, I am confirming that it accurately reflects my wishes.

________________________________________________________________________   ____/____/____
                        Signature                                           Date

If signed by personal representative:

Name of personal representative: ___________________________________________

Relationship to participant or nature of authority: ___________________________

________________________________________________________________________   ____/____/____
                        Signature of Personal Representative                  Date
FORM: GRANTING OR DENYING A REQUEST FOR RESTRICTION

Date: _____________________________________________________________

Date of Request for Restriction: ______________________________________

Name of Individual Requesting Restriction: ____________________________

☐ Your request for restriction of PHI has been accepted. You should be aware that the Plan is not required to comply with the restriction in situations when the PHI is needed for emergency medical treatment.

☐ Your request for an Use and/or Disclosure Restriction of PHI has been denied for the following reasons:

[insert reasons]

If you have privacy concerns and wish to discuss them further, please contact the undersigned.

Name of Privacy Officer: _____________________________________________

Signature of Privacy Officer: _________________________________________
An individual has the right to request that disclosures of PHI be made by alternate means or at alternate locations (a “confidential communication). The Plan will only grant such a request if the request is reasonable, in writing, and includes a clear statement that the failure to comply with the request will endanger the individual.

A request for confidential communication by a minor shall not take priority over any state law which requires the disclosure of the minor’s PHI to the minor’s parent, guardian, or person acting in loco parentis.

PROCEDURE

Requesting Confidential Communication

An individual’s request for a restriction must be in writing. The request shall include: the individual’s name and contact information; the PHI to which the request applies; the requested action by the Plan; the dates on which the requested action is to begin and end; the date of the request; a statement that the Plan’s denial of the request will endanger the individual; and the individual’s signature.

If the request is first received by a Workforce Member, the Workforce Member shall verify the identity of the individual, write the date and time of receipt on the top of the first page of the request, and forward the request to the Privacy Officer. The Workforce Member shall not tell the individual whether the Plan shall agree to the restriction.

Processing a Request for Confidential Communication

A request for a confidential communication shall be forwarded to the Privacy Officer. The Privacy Officer has the sole authority to grant or deny such requests.

Within 30 days after receipt of a request for confidential communication, the Privacy Officer shall determine whether to grant or deny the request. As soon as administratively feasible, the Privacy Officer shall communicate the determination, in writing, to the individual.

The Privacy Officer must grant the request if:

- The request is reasonable; and
- The individual has stated that the Plan’s refusal to grant the request could endanger the
individual.

The Privacy Officer shall respond to the *individual* in writing, by means and location appropriate to the request, advising the *individual* of the determination.

**When a Request for Confidential Communication Is Granted**

When the Plan agrees to a request for confidential communication, the Privacy Officer shall notify the affected Privacy Workers and *business associates*, in writing.

A notation will be made in the *individual’s* record(s).

The Plan will not *use or disclose PHI* inconsistent with the request.

**Document Retention**

The Privacy Officer shall maintain a copy of the determination and any related documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
<table>
<thead>
<tr>
<th>Name:</th>
<th>Birth Date: <em><strong>/</strong></em>/___</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>________________________</td>
</tr>
<tr>
<td>Telephone:</td>
<td>________________________</td>
</tr>
<tr>
<td>E-mail:</td>
<td>________________________</td>
</tr>
</tbody>
</table>

I hereby request that Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) communicate certain of my health information (information protected by HIPAA) in a certain way or to a particular location, as described below. I affirmatively represent that if the Plan refuses this request, I could be endangered. I understand that the Plan may deny this request if it imposes an unreasonable administrative burden.

This request applies to the following health information:

| ________________________ |
| ________________________ |
| ________________________ |

I request that the Plan communicate with me concerning this information only in the following manner and/or at the following location:

| ________________________ |
| ________________________ |
| ________________________ |

By signing this form, I am confirming that it accurately reflects my wishes.

| ________________________ | ___/___/___ |
| ________________________ | Signature | Date |

If signed by personal representative:

Name of personal representative: ________________________

| ________________________ | ___/___/___ |
| ________________________ | Signature of Personal Representative | Date |
**FORM: GRANTING OR DENYING REQUEST FOR CONFIDENTIAL COMMUNICATION**

Date: ________________________________________________________________

Date of Request: ____________________________________________________

Name of Individual Making Request: ____________________________________

☐ Your request for confidential communication has been accepted.

☐ Your request for confidential communication has been denied for the following reasons:

[insert reasons]

If you have privacy concerns and wish to discuss them further, please contact the undersigned.

Name of Privacy Officer: ______________________________________________

Signature of Privacy Officer: ___________________________________________
REQUEST FOR ACCESS TO PHI

Section: Privacy
Subsection: Individual Rights
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

An individual has the right to request access to his or her PHI that is in a designated record set and is within the Plan’s control. The Plan may deny a request for access only as set forth in these HIPAA Policies and Procedures.

PROCEDURE

Requesting Access

An individual’s request for access must be in writing. (For purposes of this Policy, “access” may be either inspection of the PHI in question or a copy of such PHI.) The request should include: the individual’s name and contact information; the PHI to which the request applies (by category or date, as the case may be); the date of the request; and the individual’s signature.

If the request is first received by a Workforce Member, the Workforce Member shall verify the identity of the individual, write the date and time of receipt on the top of the first page of the request, and forward the request to the Privacy Officer. The Workforce Member shall not tell the individual whether the Plan shall agree to the access.

Processing a Request for Access

A request for access shall be forwarded to the Privacy Officer. The Privacy Officer has the sole authority to grant or deny such requests. If the request is granted, access must generally be provided within 30 days (60 days for records maintained offsite), as more specifically provided below. Therefore, the Privacy Officer should strive to grant or deny the request within 10 days.

The 30-day and 60-day time frames referenced above may be extended once, for no more than 30 days. If the extension is necessary, the Plan shall provide the individual, within 30 days after the request, a written statement that specifies the reason(s) for the delay and the date by which the individual may expect to receive a decision on the request.

As soon as administratively feasible, the Privacy Officer shall communicate the determination, in writing, to the individual.

- The Plan may deny the individual access to any of the following PHI. Such denial is not subject to review.
  - Psychotherapy notes.
  - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or
administrative action or proceedings.

- PHI maintained by a covered entity that is subject to the Clinical Laboratory Improvement Amendments (“CLIA”), 42 USC § 263a, to the extent that access would be prohibited by law.

- PHI maintained by a covered entity that is exempt from CLIA pursuant to 42 CFR § 493.3(a)(2).

- PHI contained in records that are subject to the Privacy Act, 5 USC § 552a, if the denial meets the requirements of that law.

- PHI obtained from someone other than a health care provider under a promise of confidentiality, provided that the access would be reasonably likely to reveal the source of the information.

- The Plan may deny the individual access to PHI in any of the following circumstances. Such denial is subject to review:
  
  - A licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to endanger the life or physical safety of the individual or another person.

  - 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 requested access is reasonably likely to cause substantial harm to such other person.

  - The request for access is made by the individual’s personal representative, and a licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to cause substantial harm to the individual or another person.

- When the Plan denies access to only part of the PHI, the Plan shall provide access to the remainder of the PHI.

**When a Request for Access is Denied**

- The Plan shall provide the individual with a statement, written in plain language, that includes:
  
  - The reasons for the denial.

  - If applicable, a statement that the individual has a right to a review of the denial by a licensed health professional who is designated by the Plan but who did not participate in the original decision to deny access.

  - If applicable, the individual’s right to a review of the decision with an explanation of
how to exercise this right.

- A description of how the individual may file a complaint with the Plan and the Secretary, including the title and telephone number of the Plan’s contact person.

- If the denial is prepared by someone other than the Privacy Officer, a copy of the denial shall be forwarded to the Privacy Officer.

- To the extent possible, the Plan will grant access to other PHI for which there are no grounds to deny access.

**Reviewing A Denial of Access:**

If the denial is reviewable and the individual requests such a review:

- The Plan will designate a licensed health care professional not involved in the original denial decision, to serve as a reviewing official.

- Upon receipt of a review request, the Plan will promptly refer the denial to the reviewing official for reevaluation. The reviewer shall promptly decide whether to deny access based on the standard set forth in these HIPAA Policies and Procedures.

- The Plan will provide written notice to the individual, in plain English, of the reviewing official’s determination and shall take the steps necessary to comply with that decision. The notice will contain (i) the basis for the denial, (ii) if applicable, a statement of the individual’s review rights, including how the individual may exercise such review rights, and (iii) a description of how the individual may complain to the Plan or to the Secretary.

- If the notice is prepared by someone other than the Privacy Officer, a copy of the notice shall be forwarded to the Privacy Officer.

- If the Plan denies access because it does not maintain the PHI requested but knows where the requested PHI is maintained, the Plan will inform the individual of where to direct the request.

**When a Request for Access is Granted**

If the request for access is granted, the Privacy Officer shall notify the individual of the decision in writing.

Access to on-site records shall be provided within 30 days after receipt of the request, and access to off-site records shall be provided no later than 60 days after receipt of the request.

- The Plan shall offer access to the individual in the form of inspection, or copying, or both, as the individual may choose.

- The Plan shall produce the PHI in the form or format requested by the individual,
including electronic format, if the PHI is readable and producible in that format.

- The Plan may charge a fee for copying or other reproduction, as described below.

- In lieu of providing access, and with the agreement of the individual, the Plan may provide a summary of the requested PHI for an additional fee.

- The Plan and the individual will arrange a mutually convenient time and place for the individual to access the PHI.

**Fees**

The Plan shall charge a reasonable, cost-based fee for copying, including labor and supplies (for instance, paper, computer disks, flash drives). The Plan shall charge the cost of postage when the individual requests that the information be mailed.

No fee is charged for retrieving or handling the PHI or for processing the individual’s access request.

The Plan may charge a nominal fee for preparing an explanation or summary of the requested PHI if the individual is informed of and agrees to receive a summary of the PHI and is willing to pay the fee.

The Privacy Officer shall determine the appropriate amount of the fee, and shall inform the individual in advance so that the individual has the opportunity to elect to withdraw or modify the request to reduce or avoid the fee.

**Document Retention**

- The Plan shall maintain (or shall cause its business associates to maintain) designated record sets.

- The Privacy Officer shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
FORM: REQUEST FOR ACCESS TO PHI

Name: ___________________________________________ Birth Date: ___/___/____
Address: ____________________________________________________________
Telephone: _______________________________ Soc. Sec. # _______________________
E-mail: ____________________________________________

I hereby request a copy of my health information from the Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) for the following dates:

______________________________

and in the following records (please check one or more):
☐ Enrollment   ☐ Premium/contribution payment
☐ Customer service ☐ Case or medical management
☐ Claims, billing and EOB information relating to the following service or claim: (specify date of service and/or medical condition):

☐ Other (please specify): ____________________________________________

I would like to access my health information in the following way (please check one):
☐ Inspect and/or copy the requested information in person. (Please arrange for a mutually convenient time by calling [contact name and telephone number].) I understand I will be charged a per page copying fee of $[____].
☐ Have copies mailed to me at the following address:

________________________________________________________________________

I understand I will be charged a per page copying of $[____], plus postage.
☐ Receive a written summary of the requested information, instead of the complete records, for the fee of $[____].
☐ Other format for information or other manner of access (please specify):

________________________________________________________________________

________________________________________________________________________

Signature ___________________________ Date ___/___/____

If signed by personal representative:

Name of personal representative: ____________________________________________

Relationship to participant or nature of authority: ____________________________________________

______________________________

Signature of Personal Representative ___________________________ Date ___/___/____

4817-6164-6114.4
Dear [____],

Thank you for your request to access your health information, which was received by the Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) on [____]. Your request has been granted. Please contact me at [telephone number] to arrange for a mutually convenient time for you to inspect and/or copy the information.

If you prefer to receive a paper copy of the information by mail, please send a check payable to the Plan in the amount of $[____] to cover the costs of postage, labor, and supplies. Please include your address. We can only send the information to you, not to a third party.

If you prefer to receive a written summary of the requested information instead of a complete copy, we would be glad to prepare it for you for a fee of $[____]. Please contact me at [telephone number] if you prefer this option.

Please do not hesitate to contact me if you have any questions or require additional information.

Sincerely,
FORM: DENYING REQUEST FOR ACCESS TO PHI

Dear [_____],

Thank you for your request to access your health information, which request was received by the Trinity University Group Health Plan and/or Trinity University Flexible Benefit Plan (the “Plan”) on [______].

[Use this paragraph if denying the request in full:] After careful review, we must deny your request for any one or more of the following reason(s): [______].

[Use this paragraph if denying in part:] Your request has been granted with regard to the following records: [______]. However, after careful review, we must deny your request for access to the remaining records for any one or more of the following reason(s): [______].

[Use this paragraph if any of the reasons for the denial is subject to review:] If you believe that we have incorrectly denied you access to some or all of your health information, you have the right to request a review of our decision by contacting the Plan’s Privacy Officer in writing at [______]. We will appoint a licensed health care professional who was not involved in the original decision to reevaluate your request. You will receive a written response of the review official’s determination.

If you are dissatisfied with our decision and wish to lodge a formal complaint, you may contact the Privacy Officer or, alternatively, you may file a complaint with the Secretary of the Department of Health and Human Services.

Please contact me if you have any questions or concerns.

Sincerely,
Dear [____],

The Trinity University Group Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) received your written request for access to your PHI on [______]. Unfortunately, we will not be able to make a decision concerning your request immediately, for one or more of the following reasons: [______]

The Plan will notify you of its decision, in writing, no later than [______]. Meanwhile, if you have any questions, please contact me at [______].

Sincerely,
<table>
<thead>
<tr>
<th>REQUEST TO AMEND PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section: Individual Rights</td>
</tr>
<tr>
<td>Subsection: Right to Amend</td>
</tr>
</tbody>
</table>

## POLICY

*Individuals* have the right to request that the Plan amend incorrect or incomplete *PHI* contained in the designated record set. This right exists so long as the Plan maintains such designated record set. The Plan will decide whether to grant or deny a request for amendment within the time frames set forth in these HIPAA Policies and Procedures. The Plan may deny a request for amendment only as set forth in these HIPAA Policies and Procedures.

## PROCEDURE

### Requesting an Amendment

A request for amendment must be made in writing.

- Any *individual* who inquires about an amendment shall be advised that the request must be made in writing.

- The request shall include: the *individual’s* name and contact information; the *PHI* to which the request applies (by category or date, as the case may be); the date of the request; and the *individual’s* signature.

- If the request for amendment is not received in writing, or if the written request does not include a reason in support of the request, the Plan will not act on the request.

If the request is first received by a Workforce Member, the Workforce Member shall verify the identity of the *individual*, write the date and time of receipt on the top of the first page of the request, and forward the request to the Privacy Officer. The Workforce Member shall not tell the *individual* whether the Plan shall agree to provide the amendment.

### Processing a Request for Amendment

Only the Privacy Officer may respond to a request for amendment on behalf of the Plan.

If the Plan does not maintain the *PHI* that is the subject of the request, but knows where such *PHI* is maintained, the Privacy Officer shall inform the *individual* where to direct the request for amendment.

When a request for amendment of *PHI* is received, it will be acted on within 60 days. The Privacy Officer shall make this determination.
If necessary, the 60-day time frame may be extended for 30 days. The individual requesting the amendment will be informed in writing of the reason(s) for the delay and the date by which action will be taken on the request. The extension notice will be provided within 60 days of receipt of the original request. If the notice is prepared by someone other than the Privacy Officer, a copy of the notice shall be forwarded to the Privacy Officer.

**Grounds for Denying a Request for Amendment**

The Plan may deny amendment on any one or more of the following grounds:

- The PHI that is the subject of the request was not created by the Plan, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the request for amendment.

- The PHI that is the subject of the request is not part of a designated record set.

- The PHI that is the subject of the request would not be available for access under the Right to Access provisions of the Rule and these HIPAA Policies and Procedures.

- The PHI that is the subject of the request is accurate and complete.

**When the Request for Amendment is Denied**

The Plan will provide the individual with a written notice, in plain English, informing the individual that the request has been denied. The notice shall include all of the following:

- The basis for denial;

- A statement of the individual’s right to submit a written statement of disagreement with the denial, and instructions for filing such a statement;

- A statement explaining that if the individual does not file a statement of disagreement, the individual may nevertheless request that, when the Plan discloses the PHI in question, the Plan include the request for amendment and the denial; and

- A description of the procedure for filing a complaint with the Plan or the Secretary.

The Plan will permit the individual to file a statement of disagreement. If the individual chooses to do so:

- The statement of disagreement should include: the individual’s name and contact information; sufficient information to identify the original request for amendment; sufficient information to identify the PHI to which the statement applies; the date of the statement; and the individual’s signature.

- If the statement is first received by a Workforce Member, the Workforce Member shall verify the identity of the individual, write the date and time of receipt on the top of the first page of the request, and forward the request to the Privacy Officer. The Workforce Member
shall not tell the *individual* whether the Plan shall provide a rebuttal.

- The Plan may write a rebuttal statement, consistent with the requirements of 45 CFR § 164.526. The Plan shall provide a copy of any such rebuttal statement to the *individual*.

- In conjunction with any future *disclosure* of the *PHI* in question, The Plan will include the request for amendment, the denial notice, the statement of disagreement, and rebuttal (if any).

If the *individual* does not choose to write a statement of disagreement with the denial decision, the Plan is not required to include the request for amendment and denial decision letter with future *disclosures* of the disputed *PHI* unless requested by the *individual*.

**When the Request for an Amendment is Granted**

The Plan shall notify the *individual*, in writing, that his or her request for amendment has been granted. In that writing, the Plan shall ask the *individual* to identify the persons and entities with whom the amendment should be shared, and shall ask the *individual* for permission to share the amendment with those persons and entities.

Thereafter, the Plan shall take the following steps:

- The Plan shall identify the record(s) within its control that are the subject of the amendment request and will append the amendment to the record(s).

- Within a reasonable time, the Plan shall make reasonable efforts to make the amendment known to persons (including *business associates*) who, to the Plan’s knowledge, have received the PHI being amended and could reasonably or foreseeably rely on the un-amended PHI to the *individual’s* detriment.

- Within a reasonable time, the Plan shall make reasonable efforts to make the amendment known to the persons and entities identified by the *individual* as needing to know about the amendment, provided that the *individual* has provided permission.

**Amendments Sent to the Plan from Another Covered Entity**

The Plan may receive a notification from another *covered entity* that an *individual* has requested an amendment to *PHI* and that the request has been granted. In this event:

- The Plan shall append the amendment to all applicable records of the *individual*.

- If a *business associate* of the Plan may *use* or rely on the *PHI* that is the subject of the amendment, the Plan shall notify the *business associate* of the amendment. If the business associate maintains the designated record set that contains the PHI that is the subject of the amendment, the Plan shall direct the *business associate* to append the amendment to the relevant *PHI*. 
Document Retention

- The Contact Office is responsible for receiving requests for amendment. The Privacy Officer is responsible for processing requests for amendment.

- The Plan shall retain the amendment documents—requests for amendment, notices granting or denying amendment, statements of disagreement, and rebuttals—in the same manner and for the same length of time that it retains the designated record sets to which the amendment documents relate.

- The Privacy Officer shall maintain a copy of such requests for amendment and any related documents in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
FORM: REQUEST TO AMEND PHI

Name: ____________________________________________ Birth Date: ____/____/____
Address: __________________________________________
Telephone : ___________________ Soc. Sec. # ___________________________
E-mail:______________________________________________________

I hereby request that the Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan amend my health information (which constitutes protected health information as defined by HIPAA).

The information that needs to be amended is as follows: [_____].

The information needs to be amended as follows: [_____].

The reason for the amendment is as follows: [_____]

______________________________________________________________________  ____/____/___

Signature                                                      Date

If signed by personal representative:

Name of personal representative: _________________________________

Relationship to participant or nature of authority: ________________________

______________________________________________________________________  ____/____/___

Signature of Personal Representative                             Date
Dear [_____],

The Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) received your request to amend your health information on [______]. Your request has been granted.

If you know of any other persons (such as health care providers or other group health plans) that have your health information and need to be informed of the above amendment(s), please provide us with their names and addresses. By providing us with these names and address, you agree to allow us to provide the amendment information to these persons.

The Plan will also provide the amendment to persons that, to the Plan’s knowledge, have your health information and need the amendment in order to avoid any possible harm to you.

Please do not hesitate to contact me if you have any questions or require additional information.

Sincerely,
Dear [____],

Thank you for your request to amend your health information, which request was received by the Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) on [____].

After careful review, we must deny your request for any one or more of the following reason(s): [____].

You have the right to submit a written statement of disagreement. The statement should include the reason(s) for your disagreement with our decision. If you submit a statement of disagreement, and if the Plan later discloses the health information in question, the Plan will include a copy of the request to amend, this denial notice, and your statement of disagreement. A statement of disagreement should be sent to [____]. (Please note that the Plan has the right to place reasonable limits on the length of the statement of disagreement.)

If you choose to submit a statement a disagreement, the Plan has the right to prepare a rebuttal. If we choose to do so, you will receive a copy of it. The rebuttal will also be included with any future disclosure of the health information in question.

If you choose not to submit a statement of disagreement, you may nevertheless request that the Plan include your request to amend (and this denial letter) whenever it discloses the health information in question. Absent such a request, the Plan will not include your request or a copy of this denial letter.

If you are dissatisfied with this decision and wish to lodge a formal complaint, you may contact the Privacy Officer or, alternatively, you may file a complaint with the Secretary of the Department of Health and Human Services.

Please let me know if you have any questions or concerns.

Sincerely,
STATEMENT OF DISAGREEMENT

Name: ___________________________________ Birth Date: ____/____/____
Address: _____________________________________________
Telephone: _______________________________ Soc. Sec. # ___________________________
E-mail: _____________________________________________

I asked [_____] to amend my personal health information. My request was denied. I disagree with the denial of my request for the following reasons:

[_____]  
______________________________________________________  ____/____/____
Signature  Date

If signed by personal representative:

Name of personal representative: _____________________________________________
Relationship to participant or nature of authority: ________________________________
______________________________________________________  ____/____/____
Signature of Personal Representative  Date
Name of Individual: ____________________________ Birth Date: ___/___/____

On [____], [____] received a request to amend the above individual’s protected health information (“PHI”). On [____], this request was denied. On [____], the individual submitted a statement disagreeing with the denial.

As permitted under 45 CFR § 164.526(d)(3), [____] hereby submits this rebuttal statement.

[____]

_________________________________________  ___/___/____
Signature of Privacy Officer  Date
FORM: EXTENSION OF TIME TO DECIDE REQUEST TO AMEND PHI

Dear [_____],

Thank you for your request to amend your health information, which request was received by the Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) on [_____]. Our decision on request will be delayed.

The decision is being delayed for the following reason: [_____]

You will be notified of the decision on or before [_____].

________________________________________________________  ____/____/____
Signature of Privacy Officer  Date
RIGHT TO ACCOUNTING OF PHI DISCLOSURES

Section: Privacy
Subsection: Individual Right
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

*Individuals* have a right to an accounting of the Plan’s *disclosures* of their *PHI*. As set forth in these HIPAA Policies and Procedures, Certain *disclosures* are not required to be included in the accounting.

PROCEDURE

**Accountable Disclosures**

All *disclosures* of *PHI* are accountable *except the following*:

- *Disclosures* to carry out *treatment, payment* or *health care operations* (however, *disclosures* carry out *treatment, payment* or *health care operations* are accountable if they are made through an *electronic health record*);

- *Disclosures* made to (or for notification of) persons who are involved in an *individual’s* health care or who are involved in *payment* related to that health care;

- *Disclosures* made more than 6 years before the date of the request for accounting (3 years in the case of a *disclosure* made through an *electronic health record*);

- *Disclosures* to the *individual*, or the *individual’s* personal representative, about his own *PHI*;

- *Disclosures* incident to a *use* or *disclosure* permitted or required by the Rule;

- *Disclosures* made for disaster relief;

- *Disclosures* pursuant to an authorization;

- *Disclosures* for national security or intelligence purposes;

- *Disclosures* to correctional institutions or a law enforcement officer regarding inmates or persons in lawful custody; or

- *Disclosures* prior to April 14, 2004. [April 14, 2003 for large group health plans]

**Tracking and Logging Accountable Disclosures**

The Plan will track and log its accountable *disclosures* and will make the tracking information available to the Privacy Officer upon request so that the Plan can comply with its accounting
obligations. Likewise, the Plan will require its business associates to track, log, and provide the necessary accounting information.

The log for each accountable disclosure must include the date, name of the recipient (and address if known), description of information disclosed, and purpose for the disclosure, and if applicable a copy of the request for disclosure or the individual’s Authorization. Such record will be retained in a fashion that will allow easy access to all records affecting any single individual.

**Requests for Accounting**

A request for accounting must be made in writing.

- Any individual who inquires about an accounting shall be advised that the request must be made in writing. If applicable, the individual shall also be advised of any fees for the accounting.

- The request shall include: the individual’s name and contact information; the PHI to which the request applies (by category or date, as the case may be); the date of the request; and the individual’s signature.

- If the request for accounting is not received in writing, the Plan will not act on the request.

- If the request is first received by a Workforce Member, the Workforce Member shall verify the identity of the individual, write the date and time of receipt on the top of the first page of the request, and forward the request to the Privacy Officer. The Workforce Member shall not tell the individual whether the Plan shall agree to provide the accounting.

**Processing a Request for an Accounting**

All requests for accounting shall be forwarded to the Privacy Officer. Only the Privacy Officer may respond to a request for accounting on behalf of the Plan.

Upon receipt of a request for an accounting, the Privacy Officer shall:

- Determine if there are fees for the individual’s accounting and notify the individual of such fees in advance of compiling the accounting.

- If the request includes disclosures made by one or more business associates of the Plan, the Privacy Officer may:
  - Request the necessary information from the affected business associates and include the information provided by the business associates in the Plan’s accounting; or
  - Respond to the request with an accounting of disclosures made by the Plan and provide the individual with contact information for the business associates.

- Gather the necessary information from Privacy Workers and, where applicable, business
associates.

- Respond in writing to the individual's request within 60 days. If the Plan is unable to make its determination within such 60-day period, the Plan may obtain an extension for no more than 30 days. The Plan can obtain this extension only by providing written notice of the extension to the individual within the original 60-day period. The written notice shall explain the reason for the delay and the date by which the Plan shall provide the accounting. If the notice is prepared by someone other than the Privacy Officer, a copy of the notice shall be forwarded to the Privacy Officer.

- Forward the request for the accounting and the accounting itself to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these Privacy Policies and Procedures.

**Content of Accounting**

For each accountable disclosure of PHI, except those covered by the next paragraph, the accounting provided to the individual shall include all of the following:

- The disclosure date.
- The name and address (if known) of each person or entity that received the disclosure.
- A description of the PHI disclosed.
- A statement of the purpose of the disclosure, or, if the PHI was disclosed pursuant to a public interest or benefit activity, a copy of any written request for the disclosure from the Secretary or another government agency.

Where the Plan has made multiple disclosures to the Secretary for a single compliance review or complaint investigation, or to another government agency or organization to which the Plan disclosed PHI pursuant to a single public interest or benefit purpose, the accounting shall include the following:

- The required accounting content listed above for the first of the repetitive disclosures made within the period covered by the individual’s request.
- The frequency, periodicity, or number of the repetitive disclosures during the accounting period.
- The date of the last disclosure during the accounting period.

**Fees For Accounting**

- The Plan may not charge for an individual’s first accounting in any 12-month period.
- The Plan may charge a reasonable, cost-based fee for any subsequent accounting within that
same 12-month period.

- The Privacy Officer shall determine the amount of fees for an accounting, and shall inform the individual in advance so that the individual has the opportunity to elect to withdraw or modify the request to reduce or avoid the fee

**Suspension of an Individual’s Right to an Accounting**

The Plan must temporarily suspend an individual’s right to receive an accounting of disclosures to a health oversight agency or law enforcement official, provided that such agency or official represents (verbally or in writing) that such an accounting would likely impede the agency’s or official’s activities and indicates a specific time frame for the suspension.

If the above-described representation is made verbally, the Plan must take the following steps:

- Document the representation, including the date on which it was made, the identity of the agency or official making the representation, and the requested time frame in which the accounting should be suspended;

- Temporarily suspend the individual’s right to an accounting of disclosures subject to the representation; and

- Limit the temporary suspension to no longer than 30 days from the date of the verbal representation, unless a written statement is submitted during that time.

**Document Retention**

The Privacy Officer shall maintain the accounting documents (requests for accounting, requests for suspension, responses to such requests, and other documents regarding the Plan’s compliance with its accounting obligations) in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
FORM: REQUEST FOR ACCOUNTING OF PHI DISCLOSURES

Name: ____________________________  Birth Date: ____/____/____
Address: __________________________________________________________
Telephone: __________________________  Soc. Sec. # ______________________
E-mail: ____________________________________________________________

I hereby request an accounting of the following disclosures of my protected health information (as defined by HIPAA) made by the Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan:

Time frame for disclosures subject to this request (not to exceed 6 years from date of request or 3 years if the request is related to an electronic health record):

__________________________________________________________

Description of protected health information subject to this request:

__________________________________________________________

Description of disclosures subject to this request:

__________________________________________________________

I understand that the response to this request will not include disclosures made:

1. To carry out treatment, payment or health care operations (as those terms are defined by HIPAA), unless the disclosure was made through an electronic health record;
2. To me about my own PHI;
3. Incident to a use or disclosure that was permitted by the Privacy Rule;
4. Pursuant to an authorization;
5. For national security or intelligence purposes; or
6. To correctional institutions or a law enforcement officer.

__________________________________________________________  ____/____/____
Signature  Date

If signed by personal representative:

Name of personal representative: ________________________________________

Relationship to participant or nature of authority: ______________________________

__________________________________________________________  ____/____/____
Signature of Personal Representative  Date
Dear [_____],

On [_____], the Trinity University Group Health Plan and/or the Trinity University Flexible Benefit Plan (the “Plan”) received your request for an accounting of Disclosures. Your request has been approved.

[We have attached an accounting of the disclosures that are responsive to your request and that were made by either the Plan or its business associates. We have not included information concerning disclosures that, according to HIPAA, are not subject to the accounting requirement.]

[We have attached an accounting of the disclosures that are responsive to your request and that were made by the Plan. We have not included information concerning disclosures that, according to HIPAA, are not subject to the accounting requirement. Additional disclosures may have been made by persons who provide services to the Plan, known as the Plan’s business associates. We have attached a list of the relevant business associates, together with contact information. You may contact these persons and request an accounting directly from them.]

If you have any questions concerning the above or the attached, please feel free to contact me.

__________________________________  ____/____/______
Signature of Privacy Officer           Date
## FORM: ACCOUNTING OF PHI DISCLOSURES

For Each Accountable Disclosure:

Date of disclosure: __________________________

Name and address of person or entity to whom the disclosure was made: __________________________

Description of the PHI disclosed: __________________________

Purpose of the disclosure: __________________________

**ALTERNATE FORM**—Use only for: (1) multiple disclosures to HHS in conjunction with a single compliance review or complaint investigation; or (2) multiple disclosures to another government entity or organization, if the disclosure was made for the purpose of a public interest or public benefit:

Date of first disclosure: __________________________

Frequency or number of repetitive disclosures: __________________________

Date of last disclosure: __________________________

Name and address of person or entity to whom the disclosure was made: __________________________

Description of the PHI disclosed: __________________________

Purpose of the disclosure: __________________________
Dear [______],

On [______], [______] received your request for an accounting of certain disclosures of your PHI. After careful review, the Plan must deny your request for any one or more of the following reason(s): [______].

If you are dissatisfied with this decision and wish to lodge a formal complaint, you may contact the Privacy Officer or, alternatively, you may file a complaint with the Secretary of the Department of Health and Human Services.

Please let me know if you have any questions or concerns.

Sincerely,
<table>
<thead>
<tr>
<th>FORM: EXTENSION OF TIME TO DECIDE REQUEST FOR ACCOUNTING OF PHI DISCLOSURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dear [____],</td>
</tr>
<tr>
<td>On [_____], [____] received your request for an accounting of certain disclosures of your PHI. Our decision concerning your request will be delayed.</td>
</tr>
<tr>
<td>The decision is being delayed for the following reason: [_____]</td>
</tr>
<tr>
<td>You will be notified of the decision on or before [_____].</td>
</tr>
<tr>
<td>__________________________________________________________  <em><strong><strong>/____/</strong></strong></em></td>
</tr>
<tr>
<td>Signature of Privacy Officer  Date</td>
</tr>
</tbody>
</table>
USES AND DISCLOSURES—IN GENERAL

Section: Privacy
Subsection: Uses and Disclosures
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan will not use or disclose PHI except as permitted or required by the Rule and these HIPAA Policies and Procedures.

PROCEDURE

Most uses and disclosures are subject to the minimum necessary provisions of these HIPAA Policies and Procedures. When making a use or disclosure of PHI, a Privacy Worker shall follow any applicable minimum necessary requirements.

If the Plan has agreed to give certain PHI special privacy protections (i.e., restrictions on use and disclosure of an individual’s PHI), then any use or disclosure of the PHI is subject to the special privacy protections. When making a use or disclosure of PHI, a Privacy Worker shall follow the special privacy protection procedures set forth in the Request to Restrict Use and Disclosure Policy.

De-identified information is not PHI and may be freely used or disclosed. In creating de-identified information, and in ensuring that information is de-identified, a Privacy Worker shall follow the procedures in the De-Identified Health Information Policy.

Most disclosures of PHI must be logged for accounting purposes. Privacy Workers must log all disclosures for which an accounting is required. If there is any question as to whether a specific disclosure must be logged, the Privacy Worker shall contact the Privacy Officer, who shall be the final authority on such questions.

If there is any question as to the application of the uses and disclosures provisions, the Privacy Worker shall contact the Privacy Officer, who shall be the final authority on such questions.

Printing and Copying.

- Printed versions of PHI shall not be copied indiscriminately or left attended by a Privacy Worker.

- Printers and copiers used for printing PHI should be placed in a secure location that may not be accessed by non-Privacy Workers. If the equipment is in a location that may be accessed by non-Privacy Workers, the PHI being printed shall be strictly monitored and promptly removed when printing is complete.
Storage. PHI that is being retained but is not being used or disclosed is considered “in storage.”

- Electronic PHI that is in storage shall be protected as described in the security provisions of these HIPAA Policies and Procedures.

- Privacy Workers shall strive to keep non-Electronic PHI to a minimum.

- Non-Electronic PHI that is in storage, such as printed e-mails, shall be kept in locked file cabinets. The only persons with keys to such file cabinets shall be Privacy Workers. File rooms and other storage areas must be secured from unauthorized access.

Disposal. PHI that is not being retained, used, or disclosed shall be disposed of securely by a Privacy Worker or business associate.

- Non-Electronic PHI must not be discarded in trash bins, unsecured recycle bags or other publicly-accessible locations. Non-Electronic PHI shall be disposed of by being shredded by a Privacy Worker.

- Electronic PHI shall be disposed of as described in the security provisions of these HIPAA Policies and Procedures.
USES AND DISCLOSURES—PHI OF DECEASED INDIVIDUALS

Section: Privacy
Subsection: Uses and Disclosures

Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan protects the PHI of deceased individuals in the same manner and to the same extent as it did prior to the individual’s death.

PROCEDURE

Protection of the privacy of a deceased individual’s PHI shall be provided for a period of 50 years following the death of an individual. However, the 50-year period is not a record retention requirement and the Plan may destroy such records at the time permitted by State or other applicable law.

A personal representative of the deceased individual (someone with legal authority to act on behalf of the deceased individual or his or her estate) may exercise the deceased individual’s rights with respect to PHI.
**REQUIRED DISCLOSURES**

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Uses and Disclosures</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

### POLICY

Upon request, the Plan will *disclose PHI to the individual* that is the subject of the PHI, to, the individual’s personal representative, or to the Secretary.

### PROCEDURE

#### To the Individual

When an individual requests that PHI be disclosed to himself or herself, the Plan shall follow the procedures in the Request for Access Policy.

- When an individual requests that PHI be disclosed to another, the Plan shall not disclose the information unless the individual executes an authorization, or unless the disclosure is otherwise permitted by the Rule and these HIPAA Policies and Procedures.
- The minimum necessary requirements do not apply to these disclosures.
- The accounting requirements do not apply to these disclosures.

#### To the Individual’s Personal Representative

If the Plan would be required to disclose PHI to an individual pursuant to the above, the same disclosure is required to the individual’s personal representative, subject to proof of status as a personal representative.

- If a person seeks another individual’s PHI and claims to be the individual’s personal representative:
  - A Workforce Member shall verify the identity of the person claiming to be the personal representative.
  - A Workforce Member shall request that the person claiming to be a personal representative provide documentation that they are a legal representative of the individual and are authorized to receive the individual’s PHI.
  - The Privacy Officer shall review such documentation to ensure it complies with applicable state law.
To the Secretary

The Plan may disclose PHI to the Secretary, when required to do so by the Secretary, in order for the Secretary to investigate or determine the Plan’s compliance with the Rule. Upon a request by the Secretary:

- Any request for documents from the Secretary should be immediately forwarded to the Privacy Officer, who will be responsible for verifying the request, interacting with the Secretary, and providing the necessary documents.
- The minimum necessary requirements do not apply to these disclosures.
- The accounting requirements do not apply to these disclosures.

USES AND DISCLOSURES—PERMITTED BY THE PLAN

Section: Privacy
Subsection: Uses and Disclosures
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan shall not use or disclose PHI, except in the manner and for the purposes specifically permitted under the Rule.

PROCEDURE

To the Individual (Without a Prior Request)

The Plan may disclose an individual’s PHI to the individual at any time. However, a Privacy Worker shall not disclose an individual’s PHI, without a prior request from the individual, unless the disclosure is first approved by the Privacy Officer or is otherwise required by these HIPAA Policies and Procedures.

- The minimum necessary requirements do not apply to these disclosures.
- The accounting requirements do not apply to these disclosures.

For Treatment, Payment, and Health Care Operations (“TPO”)

The Plan may use or disclose PHI for purposes of the Plan’s treatment, payment or health care operations activities. If these HIPAA Policies and Procedures include specific procedures for a particular type of activity, then those specific procedures should be followed.

The Plan may disclose PHI to a health care provider for the treatment activities of that provider, regardless of whether the provider is a covered entity.

- The minimum necessary requirements do not apply these disclosures.
- The accounting requirements do not apply to these disclosures, unless the disclosure is made through an electronic health record.

The Plan may disclose PHI to another covered entity, or to a health care provider, for the covered entity’s or the provider’s payment activities.

- The minimum necessary requirements do not apply these disclosures.
- The accounting requirements do not apply to these disclosures, unless the disclosure is made through an electronic health record.

The Plan may disclose PHI to another covered entity for the entity’s health care operations,
provided that: (i) the entity has a relationship with the individual, (ii) the PHI pertains to that relationship, and (iii) the health care operation in question is one of the following: quality assessment and improvement, protocol development, case management and care coordination, contacting providers and patients with information about treatment alternatives, reviewing the competence or qualifications of health care professionals, evaluating health care provider performance, conducting skills training programs for professionals or health care providers, accreditation, certification, licensing, credentialing, or health care fraud and abuse detection compliance.

❖ The minimum necessary requirements apply to these disclosures.

❖ The accounting requirements do not apply to these disclosures, unless the disclosure is made through an electronic health record.

The disclosures permitted by this policy shall be subject to the provisions set forth in the Verification Policy. Additionally, the Privacy Worker making the disclosure shall take reasonable steps to verify that the recipient of PHI under this policy will be using the PHI for the stated permissible purpose.

If the Plan receives PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the Plan, the Plan may not use or disclose such PHI for any other purpose, except as may be required by law.

**Incident to a Permitted Use or Disclosure**

The Plan may use or disclose the minimum necessary PHI incident to a use or disclosure which is permitted under the Rule and by these HIPAA Policies and Procedures.

❖ The minimum necessary requirements apply to these disclosures.

❖ The accounting requirements do not apply to these disclosures.

**In Compliance with an Authorization**

The Plan may use or disclose PHI pursuant to a valid authorization. These HIPAA Policies & Procedures contain specific provisions governing authorizations.

❖ The minimum necessary requirements do not apply to these disclosures.

❖ The accounting requirements do not apply to these disclosures.

**To a Business Associate**

The Plan may disclose PHI to a business associate, and may permit a business associate to use and disclose PHI in any way that would be permitted by the Plan, provided that a valid Business Associate Agreement is in place. These HIPAA Policies & Procedures contain specific
The minimum necessary requirements apply to these disclosures, unless the specific disclosure is exempt from the minimum necessary requirements under another provision of these HIPAA Policies and Procedures.

The accounting requirements apply to these disclosures, unless the specific disclosure is exempt from the accounting requirements under another provision of these HIPAA Policies and Procedures.

To Plan Sponsor

The Plan may disclose PHI to the Plan Sponsor under any one of the following circumstances:

- The Plan has received a written authorization from the participant to disclose PHI to the Plan Sponsor;
- The PHI is information concerning an individual’s enrollment in the Plan, including whether the individual is participating in the Plan or one of the coverages within the Plan;
- The PHI is summary health information and is disclosed in order to enable Plan Sponsor (i) to obtain premium bids for providing coverage under the Plan, or (ii) to modify, amend, or terminate the Plan; or
- The PHI is disclosed in order to enable Plan Sponsor to perform Plan administration functions. Such disclosure is not permitted unless (i) the Plan document has been amended to permit such disclosure, (ii) the amendment has been certified to the Plan in accordance with 45 CFR § 164.504(f)(2); (iii) the Plan includes a separate statement in its Notice of Privacy Practices informing participants that PHI may be disclosed to the Plan Sponsor.

The accounting requirements apply to these disclosures, unless the specific disclosure is exempt from the accounting requirements under another provision of these HIPAA Policies and Procedures.

NOTE: PHI may not be disclosed to the Plan Sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor.

To Those Involved in the Individual’s Care

The Plan may use or disclose the minimum necessary PHI of an individual: (i) to a relative or other person that the individual has identified as being involved in the individual's care; (ii) to help notify a relative or other individual who is responsible for the individual's health care, of the individual's location, general condition or death; or (iii) to an authorized public or private
entity in order to assist in disaster relief efforts, or to coordinate *uses* and *disclosures* to family or other *individuals* involved in the *individual's health care*.

For any *use* or *disclosure* under this policy, the following conditions apply:

- If the *individual* is present and able to give verbal permission, the *use* or *disclosure* will only be made with such permission. This verbal permission will only cover a single encounter, and is not a substitute for a written authorization.

- If the *individual* is not present or is unable to give permission, or if an emergency makes it impractical for the Plan to seek the *individual’s* permission, the Plan will *use* or *disclose* the PHI only if it first determines (based on professional judgment) that the *use* or *disclosure* is in the *individual’s* best interest.

- The minimum necessary requirements apply to these *disclosures*.

- The accounting requirements do not apply to these *disclosures*.

- Any *disclosure* of PHI under this policy shall be subject to the Verification Policy.

**As Required by Law**

Any *disclosure* for these purposes must be authorized specifically by the Privacy Officer.

The Plan may *use* or *disclose* PHI as *required by law*, provided that the *use* or *disclosure* complies with and is limited to the relevant requirements of such law.

- The minimum necessary requirement does not apply to these *disclosures*.

- The accounting requirements generally apply to these *disclosures*.

- For *uses* and *disclosures* concerning victims of abuse, neglect, or domestic violence, follow the policies and procedures set forth below.

- For *disclosures* for judicial and administrative proceedings, follow the policies and procedures set forth below.

- For *disclosures* for law enforcement purposes, follow the policies and procedures set forth below.

**For Public Health Activities**

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may *disclose* the minimum necessary *PHI* for public health activities if any one of the following conditions exist:

- To a public health authority legally authorized to collect or receive *PHI* to prevent or control disease, injury or disability (including disease, injury, birth, death, other vital event reporting,
and public health surveillance, investigation or intervention).

- At the direction of a public health authority, to a foreign government official acting in collaboration with a public health authority.

- To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse.

- To a person subject to the jurisdiction of the FDA, with respect to an FDA-related products or activity for which that person has responsibility, for purposes related to the quality, safety, or effectiveness of such product or activity, which purposes include to: collect or report adverse events (or similar activities regarding food or dietary supplements), product, product use or labeling defects or problems, or biological product deviations; enable product recalls, repairs, replacements, or look-backs (including locating and notifying individuals who received the products); track FDA–regulated products; conduct post–marketing surveillance.

- To persons who may have been exposed to communicable disease, or are otherwise at risk of contracting or spreading disease, provided that either the Plan or a public health authority is legally authorized to give notification as needed in conducting public health intervention or investigation.

- The minimum necessary requirements apply to these disclosures.

- The accounting requirements apply to these disclosures.

**In Cases of Abuse, Neglect, or Domestic Violence**

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may disclose PHI about an individual, whom the Plan reasonably believes is or has been the victim of adult abuse, neglect or domestic violence, to a government authority (including a social service or protective service agency) legally authorized to receive reports of adult abuse, neglect or domestic violence, provided that any one of the following conditions exist:

- The disclosure is required by law or the individual agrees to the disclosure.

- The disclosure is expressly authorized by statute or regulation and the Plan (in its professional judgment) believes that the disclosure is necessary to prevent serious harm to the individual or other potential victims.

- The disclosure is expressly authorized by statute or regulation, the individual in unable to agree because of incapacity, a law enforcement official or other public official authorized to receive the report represents that (a) the PHI will not be used against the individual, and (b) an immediate enforcement activity that depends upon the PHI will be materially and adversely affected by waiting for the individual’s agreement.

- NOTE: Disclosures concerning child abuse are subject to other specific provisions of these
HIPAA Policies & Procedures.

The Privacy Officer shall notify the individual or the individual’s personal representative that it will report or has reported adult abuse, neglect or domestic violence, unless the Plan concludes, in its professional judgment, that telling the individual or the individual’s personal representative will place the individual at risk of serious harm.

❖ To the extent that disclosures under this policy are required by law, the minimum necessary requirements do not apply. However, to the extent that disclosures under this policy are not required but are permitted, the minimum necessary requirements apply.

❖ The accounting requirements apply to these disclosures.

For Health Oversight Activities

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may disclose PHI to a health oversight agency for oversight activities authorized by law, including any one or more of the following:

• Audits.
• Civil, administrative, or criminal investigations.
• Inspections.
• Licensure or disciplinary actions.
• Civil, administrative, or criminal proceedings or actions.
• Other activities necessary for appropriate oversight of: the health care system; government benefit programs for which health information is relevant to beneficiary eligibility; entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or entities subject to civil rights laws for which health information is necessary for determining compliance.

For purposes of this procedure, a health oversight activity does not include an investigation (or similar activity) when (i) the individual is the subject of the investigation, and (ii) the investigation does not arise out of, and is not directly related to: the receipt of health care; a claim for public benefits related to health; or qualification for, or receipt of, public benefits or services when a patient’s health is integral to the claim for public benefits or services.

❖ The minimum necessary requirements apply to these disclosures.

❖ The accounting requirements apply to these disclosures.

For Judicial and Administrative Proceedings
Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may disclose PHI for judicial and administrative proceedings, as permitted by 45 CFR § 164.512(e).

- The minimum necessary requirements do not apply to these disclosures.
- The accounting requirements apply to these disclosures.

For Law Enforcement Purposes

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

For law enforcement purposes, as permitted by 45 CFR § 164.512(f), the Plan may disclose PHI under any one of the following conditions:

- As required by law, including laws which require the reporting of certain injuries or wounds.

- Pursuant to legal process such as (i) a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer, (ii) a grand jury subpoena, or (iii) an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that (a) the information sought is relevant and material to a legitimate law enforcement inquiry, (b) the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (c) de-identified information could not reasonably be used.

- In response to a law enforcement official’s request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, provided that the Plan may disclose only the following information: (i) name and address, (ii) date and place of birth, (iii) social security number, (iv) blood type and factor, (v) type of injury, (vi) date and time of treatment, (vii) date and time of death, if applicable, and (viii) a description of any physical characteristics.

- In response to a law enforcement official’s request for information about an individual suspected to be the victim of a crime if (i) the individual agrees to the disclosure, or (ii) the Plan is unable to obtain the individual’s agreement because of incapacity or other emergency circumstance. The accounting requirements do not apply to these disclosures.

- To alert law enforcement official about a death, if the Plan believes that the death resulted from criminal conduct.

- To a law enforcement official concerning a crime on the Plan’s premises.

If a Workforce Member receives a written request concerning any matter covered by this policy, the Workforce Member shall write the Workforce Member’s name, and the date and time of receipt, on the top of the front page of the document, and shall forward the document to the
Privacy Officer.

If a Workforce Member receives an oral request concerning any matter covered by this policy, the Workforce Member shall immediately contact, or shall direct the requester to contact, the Privacy Officer.

- The minimum necessary requirements do not apply to these disclosures.
- Except as noted above, the accounting requirements apply to these disclosures.

**About Decedents**

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

The Plan may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the Plan may disclose the PHI prior to, and in reasonable anticipation of, the individual’s death.

- The minimum necessary requirements apply to these disclosures.
- The accounting requirements apply to these disclosures.

**For Organ, Eye, and Tissue Donation—Reserved**

**For Research—Reserved**

**To Avert a Serious Threat to Health or Safety**

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may use or disclose PHI, if the Plan, in good faith, believes the use or disclosure: is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

Similarly, the Plan may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if the Plan, in good faith, believes the use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual: because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or where it appears that the individual has escaped from a correctional institution or from lawful custody.

The Plan may use or disclose PHI under this policy only if the use or disclosure is consistent with applicable law and standards of ethical conduct.
The minimum necessary requirements apply to these disclosures.

The accounting requirements apply to these disclosures.

**Specialized Government Functions**

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may use and disclose PHI for specialized government functions, including: certain military and veterans activities; certain national security and intelligence activities; protective services for the President and others; correctional institutional and other law enforcement custodial situations.

The Plan may disclose to a correctional institution, or to a law enforcement official having lawful custody of an inmate or other individual, PHI about such inmate or individual, provided that if the correctional institution or law enforcement official represents that the PHI is necessary for any one or more of the following:

- The provision of health care to such individuals.
- The health and safety of such individual or other inmates
- The health and safety of the officers or employees of or others at the correctional institution.
- The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, Facility, or setting to another.
- Law enforcement on the premises of the correctional institution.
- The administration and maintenance of the safety, security, and good order of the correctional institution.
- NOTE: An individual is no longer an inmate, and this policy does not apply, after the individual has been released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

The minimum necessary requirements apply to these disclosures.

The accounting requirements do not apply to these disclosures.

**Workers’ Compensation**

Any disclosure for these purposes must be authorized specifically by the Privacy Officer.

The Plan may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers’ compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

To the extent that disclosures under this policy are required by law, the minimum necessary
requirements do not apply. However, to the extent that disclosures under this policy are not required but are permitted, the minimum necessary requirements apply.

❖ The accounting requirements apply to these disclosures.

**Marketing**

The Plan will not use or disclose PHI for marketing purposes.

A communication by the Plan about a product or service that encourages recipients of the communication to purchase or use the product or service is a health care operation and not marketing, provided that the Plan does not receive any direct or indirect payment from or on behalf of a third party whose product or service is being described in the communication and further provided that the communication is made:

- To describe a health-related product or service (or payment for such product or service) that is provided by the Plan, including communications about: (i) the entities participating in the Plan’s provider network; (ii) replacement of or enhancements to the Plan; and (iii) health-related products or services available only to Plan participants and beneficiaries that add value to, but are not part of, the Plan;

- For treatment of the individual; or

- For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

A communication by the Plan about a product or service that encourages recipients of the communication to purchase or use the product or service is a health care operation and not marketing, even if the Plan has received any direct or indirect payment for making the communication, provided that:

- The communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment received by the Plan in exchange for making the communication is reasonably related to the cost of making the communication; or

- The Plan obtains from the recipient of the communication a valid authorization with respect to such communication.

❖ The minimum necessary requirements apply to these disclosures.

❖ The accounting requirements apply to these disclosures.

**Fundraising**

The Plan may use or disclose limited PHI to a business associate or to an institutionally related
Foundation for fundraising purposes, provided that:

- The PHI used or disclosed is limited to demographic information, dates of service, department of service, treating physician, outcome information and health insurance status for an individual;

- The Plan’s Notice of Privacy Practices includes a statement that an individual may be contacted for fundraising purposes and that the individual has a right to opt out of receiving such communications;

- The Plan does not condition treatment or payment on the individual’s choice with respect to the receipt of fundraising communications;

- The fundraising communication provides a clear and conspicuous opportunity for the recipient to opt out of any future fundraising communications; and

- The Plan does not make fundraising communications to individuals who decide to opt out of receiving future fundraising communications.

- The minimum necessary requirements apply to these disclosures.

- The accounting requirements apply to these disclosures.
DISCLOSURES BY WHISTLEBLOWERS AND CRIME VICTIMS

Section: Privacy
Subsection: Uses and Disclosures
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

Workforce Members may disclose PHI without violating the Rule or these HIPAA Policies and Procedures, where the Workforce Members are whistleblowers or victims of a crime.

PROCEDURE

Whistleblowers

A Workforce Member may disclose PHI provided that

- the Workforce Member believes in good faith that the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Plan potentially endangers one or more patients, workers, or the public; and

- the disclosure is to:
  
  o A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plan; or

  o An attorney retained by or on behalf of the Workforce Member or business associate for the purpose of determining the legal options of the Workforce Member or business associate with regard to the conduct described in this policy.

  ▶ The minimum necessary requirements apply to these disclosures.

  ▶ The accounting requirements apply to these disclosures.

Victims of a Crime

A Workforce Member may disclose PHI provided that:

- The Workforce Member is the victim of a criminal act;

- The disclosure is made to a law enforcement official,

- The PHI disclosed is about the suspected perpetrator; and

- The PHI disclosed contains no more than the following information: name and address, date and place of birth; social security number; ABO blood type and rh factor; type of injury; date
and time of treatment; date and time of death, if applicable; and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

- The accounting requirements apply to these disclosures.
### PROHIBITION ON USE OF PHI THAT IS GENETIC INFORMATION

<table>
<thead>
<tr>
<th>Section: Privacy</th>
<th>Effective Date: September 23, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Uses and Disclosures</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

Neither the Plan nor the Plan Sponsor nor any *business associate* of the Plan shall use or disclose *PHI* that is *genetic information* for underwriting purposes.

**PROCEDURE**

With the exception of long-term care policies, the Plan shall not use or disclose *PHI* that is *genetic information* for underwriting purposes. Underwriting generally includes the following:

- Rules for, or determination of, eligibility (including enrollment and continued eligibility) form, or determination of, benefits under the Plan (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

- The computation of premium or contribution amounts under the Plan (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

- The application of any pre-existing condition exclusion under the Plan; and

- Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.
PROHIBITION ON SALE OF PHI

Section: HITECH
Subsection: n/a
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

Neither the Plan nor any business associate of the Plan shall directly or indirectly receive remuneration in exchange for any PHI of an individual except as permitted by this Policy.

PROCEDURE

The Plan shall not receive direct or indirect remuneration from or on behalf of the recipient of the PHI in exchange for the PHI, unless the sale and remuneration are authorized by the individual whose PHI is to be sold or an exception under the Rule applies.

The Plan’s form business associate agreement shall prohibit the business associate from receiving direct or indirect remuneration from or on behalf of the recipient of the PHI, unless the sale and remuneration are authorized by the individual whose PHI is to be sold or an exception under the Rule applies.

Authorizations for the sale of PHI must specifically state that the Plan is receiving remuneration in exchange for the PHI and whether the PHI may be further exchanged for remuneration by the recipient of the PHI.

The exchange of PHI for remuneration is not subject to the prohibition or authorization requirement, provided that:

- The purpose of the exchange is for public health activities;

- The purpose of the exchange is for any disclosure permitted by the Rule and the price charged reflects a reasonable cost-based fee to cover the cost to prepare and transmit the data for such purpose;

- The purpose is for the sale, transfer, merger, or consolidation of all or part of a covered entity and related due diligence, if the recipient will become a covered entity;

- The purpose of the exchange is for treatment and payment, subject to any regulation that the Secretary may promulgate to prevent PHI from inappropriate access, use, or disclosure;

- The purpose of the exchange is for remuneration that is provided by the Plan to a business associate for activities involving the exchange of PHI that the business associate undertakes on behalf of and at the specific request of the Plan pursuant to a business associate agreement, and the only payment provided by the Plan to the business associate is for the...
performance of such activities;

- The purpose of the exchange is to provide an *individual* with access to or an accounting of the *individual’s PHI*;

- The purpose is *Required by Law*; or

- The purpose of the exchange is otherwise determined by the *Secretary* in regulations to be similarly necessary and appropriate as the other exceptions.
POLICY

In the event of a HIPAA Breach, the Privacy Officer shall provide notification, as required by the following procedure, to each individual whose Unsecured PHI was subject to the Breach, to the Secretary, and as applicable, to the media.

PROCEDURE

If any Workforce Member discovers a potential HIPAA Breach, the Workforce Member shall immediately alert the Privacy Officer. The Privacy Officer shall conduct an investigation to determine whether a HIPAA Breach occurred. If the Privacy Officer determines that a HIPAA Breach occurred, the following notification procedures shall apply.

Notice to Individuals

The Privacy Officer shall send written notice to any individual whose PHI was the subject of the HIPAA Breach.

- The notice shall be provided without unreasonable delay and in any event no later than 60 days after the HIPAA Breach is discovered. The Plan shall treat a HIPAA Breach as “discovered” as of the first day on which the HIPAA Breach was known (or should reasonably have been known) by the Plan or by a Workforce Member, not including the individual committing the HIPAA Breach.

- Notice shall be provided by first class mail to the individual at the last known address of the individual (or, if the individual is deceased, to the next of kin). If the individual or next-of-kin agrees, electronic notice may be provided in lieu of written notice.

- If the Plan has insufficient or out-of-date contact information that precludes direct notification to the individual, a substitute form of notice reasonably calculated to reach the individual may be provided.

- If there are ten or more individuals for whom the Plan has insufficient or out-of-date contact information, substitute notice is required. For these purposes, substitute notice must consist of: a conspicuous notice on the home page of the Plan’s web site, or in major print or broadcast media in geographical areas where the affected individuals likely reside. The conspicuous notice must be posted for at least 90 days and must include a toll-free phone number where an individual can learn whether his or her PHI was affected by the HIPAA Breach.

- Where the Plan determines a HIPAA Breach requires urgency because of possible imminent
misuse of *Unsecured PHI*, the Privacy Officer, in addition to written notice, may provide information to *individuals* by telephone or other means, as appropriate.

**Notice to the Media**

If a HIPAA Breach involves the *Unsecured PHI* of 500 or more *individuals*, the Privacy Officer shall notify prominent media outlets serving the State or jurisdiction.

The notice shall be provided without unreasonable delay and in any event no later than 60 days after the HIPAA Breach is discovered.

**Notice to the Secretary**

The Privacy Officer shall provide notice of all HIPAA Breaches to the *Secretary*.

- If the HIPAA Breach affects less than 500 *individuals*, the Privacy Officer shall make an appropriate entry in the Plan’s log. The Privacy Officer shall submit the log annually to the *Secretary*. The log for a given calendar year shall be submitted no later than 60 days after the end of the calendar year in which the HIPAA Breach was discovered, in a manner specified on the HHS website, or as the *Secretary* may otherwise require.

- If the HIPAA Breach affects 500 or more *individuals*, then in addition to the foregoing, the Privacy Officer shall provide notice to the *Secretary* at the same time that notice is provided to the affected *individuals*.

**Content of the Notice**

The notice required by this Policy shall include, to the extent possible:

- A brief description of what happened, including the date of the HIPAA Breach and the date of the discovery of such HIPAA Breach, if known;

- A description of the types of *Unsecured PHI* that were involved in the HIPAA Breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information involved);

- The steps *individuals* should take to protect themselves from potential harm resulting from the HIPAA Breach;

- A brief description of what the Plan is doing to investigate the HIPAA Breach, to mitigate losses, and to protect against any further HIPAA Breaches; and

- Contact procedures for *individuals* to ask questions or learn additional information; including a toll free telephone number, an e-mail address, Web site, or postal address.

**Law Enforcement Delay**
The Plan shall delay a notice otherwise required by this Policy, if a law enforcement official states (verbally or in writing) to the Plan that the notice would impede a criminal investigation or cause damage to national security. A delay under this paragraph shall be approved by the Privacy Officer, who shall be responsible for ensuring adherence to the following conditions:

- The Plan shall verify the identity of the law enforcement official.
- If the statement is in writing and specifies the time for which the delay is required, the Plan shall delay for the specified time.
- If the statement is made verbally, the Plan shall delay for no longer than 30 days, unless a written statement is submitted during that time.

**Document Retention**

The Privacy Officer shall ensure that any notices distributed pursuant to this policy are maintained in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures. In addition, the Privacy Officer shall establish the timeliness of the notices and, where applicable, why the Plan determined that a notice was not required.
ASSIGNED SECURITY RESPONSIBILITY

<table>
<thead>
<tr>
<th>Section: Security</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Administrative Safeguards</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

**POLICY**

The Plan shall have a Security Officer, whose name and contact information will be documented in these HIPAA Policies and Procedures. The Security Officer is responsible for the development and implementation of the Plan’s policies and procedures that are designed to protect the confidentiality, integrity and availability of electronic PHI. The Security Officer is also responsible for overseeing the Plan’s compliance with the Rule.

**PROCEDURE**

*Selection of Security Officer*

The Security Officer is selected by the Vice President for Information, Marketing & Communications and the Director & Chief Information Technology Officer, which shall review the selection as needed.

*Delegation of Duties By Security Officer*

The Security Officer may delegate his or her duties or responsibilities to one or more Workforce Members. However, if the duty or responsibility in question involves the use or disclosure of electronic PHI, the duty or responsibility may be delegated only to a Privacy Worker.

*Documenting the Security Officer*

The name and contact information of the Security Officer are as follows:

Stephen Perez  
Information Security Administrator  
Trinity University  
One Trinity Place  
San Antonio, TX 78212-7200  
(210) 999-7619  
sperez@trinity.edu

A written copy of this and all subsequent designations of the Security Officer, including the effective date of such designation(s), shall be forwarded to the Privacy Officer, who shall maintain a copy of the designation in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.

*Essential Duties and Functions of the Security Officer*
• Implement administrative, physical and technical safeguards (as defined below) to ensure the confidentiality, integrity and availability of electronic PHI.

• Develop and implement security policies and procedures in accordance with the Rule and all other applicable laws;

• Provide leadership and assume accountability for the Plan's compliance with the HIPAA Security Policies and Procedures;

• Delegate responsibility for security-related matters as needed and appropriate;

• Coordinate risk assessment and risk management activities to ensure ongoing identification of threats to the confidentiality, integrity and availability of electronic PHI and selection of appropriate safeguards to manage and reduce risks;

• Ensure that operations comply with the security policies and procedures;

• Ensure that security policies, procedures, and practices are revised as needed;

• Review all security incidents and ensure that response and reporting procedures are followed and that harm caused by security incidents is mitigated to the extent practicable;

• Assist in determining whether a HIPAA Breach occurred and notify the Privacy Officer of same;

• Cooperate with oversight agencies in any investigations of security violations;

• Develop and conduct training on and foster awareness of security policies and procedures to ensure that all Workforce Members, including management, receive adequate and appropriate security training; and

• Serve as an internal and external liaison and resource with outside entities (including business associates, technology vendors, trustees, and other parties) to ensure that the Plan’s security practices are implemented, consistent and coordinated.

Administrative Safeguards

Those actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI and to manage the conduct of Workforce Members in relation to the protection of an authorized access to electronic PHI.

Physical Safeguards

Those physical measures, policies and procedures to protect the Plan’s electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Technical Safeguards
The technologies and the policies and procedures that protect *electronic PHI* and to control access to such *electronic PHI.*
POLICY

The Plan shall conduct a risk assessment to determine potential threats to the confidentiality, integrity and availability of electronic PHI.

PROCEDURE

The Security Officer shall be responsible for conducting, and periodically reviewing a Risk Analysis. Specifically, the Security Officer shall ensure that the Plan:

- Understands the technical and non-technical components of its security environment related to electronic PHI;
- Reviews the standards and implementation specifications of the Rule;
- Conducts a Risk Analysis that evaluates the Plan’s compliance against the standards and implementation specifications; and
- Produces a written Risk Analysis and Management Report which summarizes the result of the analysis.

- The Security Officer shall ensure that the Risk Analysis and Management Report is reviewed periodically to audit the Plan's continued compliance with the Rule and its effectiveness in reducing security risks.

Conducting the Risk Analysis

The Security Officer shall appropriately assess the potential vulnerabilities associated with storing electronic PHI, transmitting electronic PHI internally among Privacy Workers and transmitting electronic PHI externally. The Security Officer shall:

- **Identify and document all electronic PHI repositories.** All repositories will be identified and logged into a common catalogue. An electronic PHI repository may be in the form of a database, spreadsheet, folder, storage device, document or other form of electronic information that is accessed by one or more Privacy Workers. Each repository will be logged with the appropriate level of file, system and owner information, including but not limited to, (i) repository name, (ii) custodian contact information, (iii) number of records, (iv) system name, (v) system IP address, (vi) system location, (vii) system manager contact information, (viii) users that access the repository, and (ix) risk level.

- **Periodically re-inventory electronic PHI repositories.** The Security Officer shall ensure
that the *electronic PHI* inventory is updated at least annually to ensure that the *electronic PHI* catalogue is up to date and accurate.

- **Identify the potential vulnerabilities to each *electronic PHI repository***. Each *electronic PHI* repository will be analyzed for any potential vulnerability to the integrity, confidentiality and availability of the *electronic PHI*. The Security Officer shall ensure that the potential risks and vulnerabilities to the integrity, confidentiality and availability of each *electronic PHI* repository are reassessed at least annually.

- **Assign a level of risk to each *electronic PHI repository***. The Security Officer shall ensure that the level of risk assigned to each *electronic PHI* repository is reassessed at least annually.

- **Mitigation**. The Security Officer shall take appropriate action to eliminate or mitigate any vulnerabilities discovered as a result of the Risk Analysis.

The Security Officer shall ensure that the Risk Analysis and Management Report is forwarded to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
## RISK MANAGEMENT

<table>
<thead>
<tr>
<th>Section: Security</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Administrative Safeguards</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

### POLICY

The Plan selects and implements security measures sufficient to reduce risks to the confidentiality, integrity and availability of electronic PHI to a reasonable and appropriate level.

### PROCEDURE

The Risk Analysis performed by the Plan shall identify the risks and vulnerabilities of the Plan’s electronic PHI.

The Security Officer shall ensure that appropriate personnel decide how to manage those risks and vulnerabilities. Such decision shall take into consideration the Plan’s size, complexity, and technical capabilities, as well as the costs of security measures relative to the reduction in risk.

The Security Officer shall implement security measures to reduce risks and vulnerabilities for each electronic PHI repository to a reasonable and appropriate level in order to:

- Ensure the confidentiality, integrity and availability of all electronic PHI the Plan creates, receives, maintains or transmits;
- Protect against any reasonable anticipated threats or hazards to the security or integrity of electronic PHI;
- Protect against any impermissible uses or disclosures of electronic PHI;

Low-risk electronic PHI repositories may be appropriately safeguarded using security measures such as user accounts, passwords, and perimeter firewalls. More extensive safeguards must be utilized for medium and high-risk electronic PHI repositories.

The Plan shall document its risk management decisions in the Risk Analysis and Management Report. The Security Officer shall ensure that the Risk Analysis and Management Report is reviewed periodically to audit continued effectiveness of the Plan's risk management choices.

The Security Officer shall ensure that the Risk Analysis and Management Report is forwarded to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
POLICY

The Plan will apply sanctions against Privacy Workers who fail to comply with the Plan’s security policies.

PROCEDURE

- Sanctions for violations of the Plan’s security policies shall be determined and imposed through the ordinary disciplinary process established by Plan Sponsor, except as set forth in the remainder of this paragraph. For any violation of the Plan’s security policies, to the extent that the ordinary disciplinary process does not already include the Security Officer, the Security Officer shall become an integral part of such process. If the ordinary disciplinary process calls for the final determination on discipline to be made by a Workforce Member (such as the Human Resources Director), the final determination on discipline for a violation of these HIPAA Policies and Procedures shall be made by or in consultation with the Security Officer.

- Sanctions shall be applied against any Workforce Member who violates the Plan’s security policies. The sanction shall be determined based on the nature of the violation, its severity, and whether it was intentional or unintentional. Sanctions may include verbal warnings, written warnings, probationary periods with or without pay, alteration in duties / job reassignment, or termination of employment, as well as civil or criminal liability.

- In the event that sanctions are imposed, the Security Officer shall write a report, which shall include, at a minimum: the name of the Workforce Member; the nature of the security violation; and the sanction imposed. A copy of the report shall be forwarded to the Privacy Officer, who shall maintain the report in a file specifically designated for such reports. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.

- Sanctions shall not be applied against Workforce Members who file a complaint concerning a violation of these HIPAA Policies and Procedures or of the Rule. Sanctions shall not be applied against Workforce Members who refuse to follow a policy or procedure that they believe, in good faith, violates the Rule.
## FORM: SANCTION LOG

<table>
<thead>
<tr>
<th>Date of Violation: [_____]</th>
<th>Date of Sanction: [_____]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Name:** ________________________________

**Title:** ________________________________

**Description of violation:**

<table>
<thead>
<tr>
<th>Description of sanction issued:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Summary** (Describe whether the violation resulted in a threat to the confidentiality, integrity and availability of *electronic PHI*, if so what steps have been taken to correct this specific violation and to prevent future violations.)

<table>
<thead>
<tr>
<th>Security Official Signature/Date: ________________________________</th>
</tr>
</thead>
</table>
# INFORMATION SYSTEM ACTIVITY REVIEW

<table>
<thead>
<tr>
<th>Section: Security</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection: Administrative Safeguards</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
</tbody>
</table>

## POLICY

The Plan will review records of information system activity on a regular basis in order to prevent, detect, correct and contain security violations.

## PROCEDURE

The Security Officer is responsible for coordinating the review of records of information system activity including, but not limited to, reviews of audit logs, access reports, and security incident tracking reports.

- An internal audit procedure is used to regularly review records of system activity. The internal audit procedure may utilize audit logs, activity reports, or other mechanisms to document and manage system activity.

- Audit logs, activity reports, or other mechanisms to document and manage system activity must be reviewed at intervals commensurate with the associated risk of the information system or the electronic PHI repositories contained on the information system. The interval of system activity review must not exceed, but may be less than one year.

- An audit control and review plan shall include (i) the systems and applications to be logged, (ii) information to be logged for each system, and (iii) procedures to review all audit logs and activity reports.

- Security incidents such as activity exceptions and unauthorized access attempts must be detected, logged and reported immediately to the Security Officer.

The Plan will use the records of information system activity as needed and appropriate to investigate root causes of suspected security incidents or other security violations.

The Plan will provide Workforce Members periodic reminders that computer access activity is reviewed regularly.
## POLICY

The Plan's security policies shall be designed to ensure that all Workforce Members have appropriate access to *electronic PHI* and to prevent those Workforce Members who are not entitled to access from obtaining access to *electronic PHI*.

## PROCEDURE

### Authorization and/or Supervision [Addressable]

Workforce Members shall be given access to *electronic PHI* only upon the written approval of the Security Officer.

Workforce Members who do not require access to *electronic PHI* shall not work in areas where *electronic PHI* is stored, except upon the written approval of the Security Officer.

Non-Workforce Members who work with *electronic PHI* or in areas where it may be accessed (including both maintenance and operations workers) must receive appropriate authorization from the Security Officer and/or supervision while onsite.

Periodic access reviews will be conducted by information technology personnel.

### Workforce Clearance Procedures [Addressable]

The hiring practices of the Plan Sponsor include reference checks and other appropriate mechanisms so that access to *electronic PHI* is not granted to individuals who represent security risks.

The Security Officer periodically reviews Workforce Members’ access to *electronic PHI* in order to confirm that the access rights are appropriate in light of changing job duties, skills, and experiences.

The Security Officer, in connection with information technology personnel, shall ensure that access to *electronic PHI* is protected utilizing such measures as workstation access, password protection, virus protection software, transaction and program access controls and other appropriate mechanisms.

The Security Officer will be responsible for periodic audits to ensure that access protection devices are functioning properly, including but not limited to, (i) periodic reviews of log-in attempts and discrepancy reporting, (ii) periodic reviews to ensure that passwords are appropriately created, changed and safeguarded, and (iii) periodic review of remote access to the
Plan’s *electronic PHI*.

**Termination Procedures [Addressable]**

Upon termination of a Workforce Member’s employment, the Security Officer shall complete a Termination of Access Checklist and shall terminate the Workforce Member’s access to all *electronic PHI*, the Plan’s information systems, and the buildings housing Plan information (electronic or otherwise). Access may be terminated earlier if circumstances so require.

Human Resources personnel will notify the Security Officer (or other appropriate information technology personnel) when a Workforce Member’s employment terminates. The Security Officer shall complete a Termination-of-Access Checklist and shall terminate the Workforce Member’s access to all *electronic PHI* as soon as practicable when a Workforce Member’s employment terminates.

When a Workforce Member no longer needs access to *electronic PHI* as part of their job duties and responsibilities, Human Resources personnel or the Workforce Member’s supervisor will notify the Security Officer (or other appropriate information technology personnel) when access is no longer required. The Security Officer shall complete a Termination-of-Access Checklist and shall terminate the Workforce Member’s access to all *electronic PHI* as soon as practicable when a Workforce Member’s job duties change.
<table>
<thead>
<tr>
<th>FORM: TERMINATION-OF-ACCESS CHECKLIST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Employee:</strong></td>
</tr>
<tr>
<td><strong>Date and time by which access privileges must be revoked:</strong></td>
</tr>
<tr>
<td><strong>Reason for termination of access privileges:</strong></td>
</tr>
<tr>
<td>☐ Employee has resigned</td>
</tr>
<tr>
<td>☐ Employee has been terminated</td>
</tr>
<tr>
<td>☐ Access privileges no longer appropriate for job duties</td>
</tr>
<tr>
<td><strong>Administrative</strong></td>
</tr>
<tr>
<td>☐ Information systems access lists – delete name from list</td>
</tr>
<tr>
<td><strong>Physical</strong></td>
</tr>
<tr>
<td>Retrieve the following items. Alternatively, deactivate the item or change the “lock” that would be opened by the item.</td>
</tr>
<tr>
<td>☐ Identification Badge</td>
</tr>
<tr>
<td>☐ Access codes</td>
</tr>
<tr>
<td>☐ Keys</td>
</tr>
<tr>
<td>☐ Pager</td>
</tr>
<tr>
<td>☐ Cell phone</td>
</tr>
<tr>
<td>☐ Laptop</td>
</tr>
<tr>
<td>☐ PDA</td>
</tr>
<tr>
<td><strong>Technical</strong></td>
</tr>
<tr>
<td>☐ User account and access privileges – revoke</td>
</tr>
<tr>
<td><strong>Signature:</strong></td>
</tr>
<tr>
<td><strong>Printed Name:</strong></td>
</tr>
<tr>
<td><strong>Date and Time:</strong></td>
</tr>
<tr>
<td>INFORMATION ACCESS MANAGEMENT</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Section: Security</td>
</tr>
<tr>
<td>Subsection: Administrative Safeguards</td>
</tr>
</tbody>
</table>

**POLICY**

Access to *electronic PHI* is authorized, established, maintained and modified based on the minimum amount of *PHI* necessary for individual Workforce Members to perform their jobs effectively.

**PROCEDURE**

*Isolating Health Care Clearinghouse Functions [Required]*

Not applicable.

*Access Authorization [Addressable]*

Workforce Members shall be given access to *electronic PHI* only upon the written approval of the Security Officer. Workforce Members shall be given access to the minimum amount of *electronic PHI* necessary to perform his or her job effectively.

*Access Establishment and Modification [Addressable]*

After access has been authorized, a user account is established that enables a Workforce Member to access *electronic PHI* and the Plan’s information systems as appropriate to his or her job function.

The Security Officer shall maintain lists of user accounts and access privileges and shall review the user accounts and access privileges at regular intervals to ensure continued appropriateness. Periodic audits will be conducted by information technology personnel to ensure that employee access to *electronic PHI* is appropriate given the Workforce Member’s job responsibilities.

Supervisors shall keep the Security Officer informed of job function changes that might require an increased or decreased level of access privileges. The Security Officer shall modify or revoke user accounts and access privileges whenever a Workforce Member’s job function changes, as deemed appropriate by the Security Officer.
POLICY

The Plan provides a security awareness and training program for all Workforce Members, including management.

PROCEDURE

Training

Workforce Members, including management, receive security training upon employment (prior to obtaining access to electronic PHI), when their job duties change, and whenever there are material changes to the Plan’s security environment. The training includes information concerning security generally, HIPAA security requirements, and these security policies. Additional details concerning the training are set forth in the remainder of this Policy. The depth of training shall be commensurate with the Workforce Members’ job duties.

Security Reminders [Addressable]

The Security Officer will send periodic security reminders to Workforce Members, including management, to ensure awareness of security issues and concerns related to PHI.

Protection From Malicious Software [Addressable]

The Security Officer trains all new hires in guarding against, detecting, and reporting malicious software. The Security Officer provides refresher training at reasonable intervals for existing Workforce Members. The Security Officer provides periodic security reminders to Workforce Members concerning responsibilities with respect to guarding against, detecting and reporting malicious software.

Anti-virus software with current virus definition files is installed on all desktops, laptops and servers and programmed to conduct automatic virus scanning. Security patches and updates for computer operating systems and software are installed to reduce known vulnerabilities.

Workforce Members are not allowed to download software from the Internet or install software on desktops or laptops.

Workforce Members are warned against opening e-mail attachments from unknown or untrustworthy sources. All e-mail attachments from known and trustworthy sources must be scanned for the presence of viruses.

If a Workforce Member detects or suspects a virus, the Workforce Member must promptly notify
the Security Officer. Workforce Members are not allowed to proceed with virus eradication efforts without authorization and supervision. If a machine is (or is suspected of being) contaminated with a virus, the Security Officer must ensure that the machine is isolated from the network and not reconnected to the network until it has been scanned, cleaned, and repaired.

**Log-in Monitoring [Addressable]**

The Security Officer trains all new hires in guarding against, detecting, and reporting malicious software. The Security Officer provides refresher training at reasonable intervals for existing Workforce Members.

The Security Officer receives periodic reports of unsuccessful log-in attempts and investigates all suspicious attempts.

**Password Management [Addressable]**

The Security Officer trains all new hires in establishing and maintaining strong and secure passwords. The Security Officer provides refresher training at reasonable intervals for existing Workforce Members.

Workforce Members are required to create strong passwords for user accounts, e-mail and screensaver protection.

- Passwords must contain at least eight (8) characters long and contain three (3) of the following: (i) any lower case letters (a-z), (ii) any upper case letters (A-Z), (iii) any numbers (0-9), and (iv) any punctuation or non-alphanumeric characters found on a standard ASCII keyboard.

- Passwords may not be based on personal information such as nicknames, family names, birth dates or other information that may be easily guessed.

- Passwords must not be words found in a dictionary.

- Passwords must be created that are easily remembered.

- Group passwords are not allowed.

- The use of control characters and other non-printing characters is prohibited.

- Workforce Members shall not disclose their passwords to others, except to the Security Officer or information technology staff as necessary for system management.

Workforce Members are required to change their passwords:

- At least once every sixty (60) days.

- In the event that the password is suspected of being disclosed, or known to have been disclosed to unauthorized parties.
If a Workforce Member has been terminated or resigns, his or her password must be deleted within twenty-four (24) hours of the termination or resignation date listed in his or her employment file.

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three (3) unsuccessful attempts to enter a password, the Workforce Member’s password must be either (i) suspended until reset by a system administrator; (ii) temporarily disabled for no less than three (3) minutes, or (iii) if dial-up or other external network connections are involved, disconnected.

Previous passwords may not be reused.

Workforce Members are not allowed to write down their passwords or keep them close to their workstation (for example, on Post-it notes affixed to monitors or keyboards).

**Document Retention**

All training referenced in this Policy shall be documented. The documentation shall include the date of the training, the name of the trainer, a summary of the training, and the names of the persons trained. The documentation shall be forwarded to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
<table>
<thead>
<tr>
<th>Date of Training:</th>
<th>Name of Trainer:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Summary of Topic Covered**

<table>
<thead>
<tr>
<th>Employee Name (Printed)</th>
<th>Employee Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SECURITY INCIDENTS

<table>
<thead>
<tr>
<th>Section: Security</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsection:</td>
<td>Last Reviewed On: September 23, 2013</td>
</tr>
<tr>
<td>Administrative Safeguards</td>
<td></td>
</tr>
</tbody>
</table>

**POLICY**

The Plan identifies and responds to suspected or known security incidents. The Plan mitigates, to the extent practicable, harmful effects of any security incidents that are known to the Plan. The Plan documents security incidents and the responses thereto.

**PROCEDURE**

Workforce Members shall report all suspected or actual security incidents to the Security Officer as soon as practicable.

The Security Officer shall immediately document the report on an Security Incident Report Form. Thereafter:

- The Security Officer shall conduct an investigation of the suspected security incident.
- If the Security Officer determines that the security incident resulted in a potential HIPAA Breach, the Security Officer shall immediately notify the Privacy Officer.
- The Security Officer shall determine an appropriate response to the security incident. The Security Officer may involve other personnel in the determination. The response shall be based upon the nature and severity of the security incident. Responses may include, but shall not be limited to, the application of sanctions, initiation of security reminders, additional training or an evaluation of the adequacy of security measures. The response shall include the mitigation (to the extent practicable) of harm caused to any individual by the security incident.
- The Security Officer shall document the response on the Security Incident Log.

The Security Officer shall review the Security Incident Log on a periodic basis to determine and ensure the adequacy of security measures and compliance with the Rule.

**Document Retention**

The Security Officer shall forward the security incident documentation—the Security Incident Report, the paperwork relating to any investigation of a suspected security incident, and the Security Incident Log—to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
<table>
<thead>
<tr>
<th>Form: Security Incident Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Person Reporting Incident</strong></td>
</tr>
<tr>
<td><strong>Name:</strong></td>
</tr>
<tr>
<td><strong>Phone:</strong></td>
</tr>
<tr>
<td><strong>Date and time of report:</strong></td>
</tr>
<tr>
<td><strong>Type of security incident (check the appropriate box):</strong></td>
</tr>
<tr>
<td>☐ Unauthorized access</td>
</tr>
<tr>
<td>☐ Unauthorized use or disclosure</td>
</tr>
<tr>
<td>☐ Unauthorized modification of data</td>
</tr>
<tr>
<td>☐ Theft of equipment</td>
</tr>
<tr>
<td>☐ Loss of equipment</td>
</tr>
<tr>
<td>☐ Unattended workstation</td>
</tr>
<tr>
<td>☐ Software malfunction</td>
</tr>
<tr>
<td>☐ System failure</td>
</tr>
</tbody>
</table>

Provide a brief description of the security incident including persons and equipment involved:

| **Signature:** | **Date:** |
### FORM: SECURITY INCIDENT LOG

**Person Reporting Incident**

<table>
<thead>
<tr>
<th>Name:</th>
<th>Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone:</td>
<td>E-Mail:</td>
</tr>
</tbody>
</table>

**Date and time of report:**

**Date and time of security incident:**

**Description of security incident:**

**Description of investigation:**

**Did a HIPAA Breach occur as a result of the security incident?**

**If so, on what date was the Privacy Officer notified?**

**Description of response:**

**Description of any harm to an individual and mitigation of such harm:**

<table>
<thead>
<tr>
<th>Security Official Signature:</th>
<th>Date:</th>
</tr>
</thead>
</table>
CONTINGENCY PLAN

Section: Security
Subsection: Administrative Safeguards
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan maintains a contingency plan. The contingency plan contains policies and procedures to enable the Plan respond to an emergency, disaster or other occurrence that damages systems containing *electronic PHI*.

PROCEDURE

The Security Officer shall coordinate the preparation of a written contingency plan for the Plan’s *electronic PHI*. The Security Officer shall assess the criticality of applications and data at least annually to ensure that appropriate procedures are in place for data and applications based on the respective level of risk associated with the *electronic PHI*.

The contingency plan shall include each of the following:

- **Data backup plan** [*Required*]. Procedures to create and maintain retrievable exact copies of *electronic PHI*. The data backup plan shall apply to all files, records, images, voice or video files that contain *electronic PHI*. The data backup plan shall require that all media used for backing up *electronic PHI* be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on-site, in a physically secure location, different from the Location of the Plan’s information systems. If an off-site storage facility or backup service is used, a Business Associate Agreement is required with the service provider.

- **Disaster recovery plan** [*Required*]. Procedures to restore and recover any *electronic PHI* lost in a disaster and the systems needed to make the *electronic PHI* available in a timely manner. The disaster recovery plan shall include (i) procedures to restore *electronic PHI* from data backups in the case of a disaster causing data loss, and (ii) procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

- **Emergency mode operation plan** [*Required*]. Procedures to enable continuation of critical business processes for protection of the security of *electronic PHI* while operating in emergency mode.

- **Testing and revision procedures** [*Addressable*]. Procedures for periodic testing and revision of all elements of the contingency plan.

- **Identify Preventative Measures** [*Required*]. Procedures for identifying preventative measures which are deemed practical and feasible in the Plan’s given environment.
• **Applications and data criticality analysis [Addressable].** Procedures for assessing the relative criticality of specific applications and data in support of the other contingency plan components.

The Security Officer shall be responsible for conducting an analysis of applications and data which are critical to the support of other contingency plan components. Copies of the contingency plan for *electronic PHI* shall be maintained off-site in secure, accessible locations.

Workforce Members shall receive training concerning the contingency plan, to the extent appropriate for their job duties.

**Document Retention**

The Security Officer shall forward a copy of the contingency plan to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
POLICY

The Plan shall perform a periodic technical and nontechnical evaluation of its administrative safeguards to determine the extent to which the security policies meet the Rule's requirements.

PROCEDURE

The initial evaluation of the Plan’s security environment and its compliance with the Rule shall be addressed under the Risk Analysis and Risk Management Policies.

Thereafter, the Security Officer, in conjunction with Internal Audit, shall conduct periodic technical and nontechnical evaluation of the Plan’s security policies and procedures to determine the extent to which they meet the Rule's requirements.

- An evaluation shall be conducted no less than every three (3) years.
- An evaluation shall be conducted whenever there are technological, environmental or operational changes that, in the opinion of the Security Officer, affect the security of the Plan’s electronic PHI.
- Internal Audit shall be responsible for notifying the Security Officer concerning the results of any evaluation.
- The Security Officer shall be responsible for correcting any deficiencies noted during the course of the evaluation and the Security Officer shall certify that any deficiencies have been corrected. This certification shall take into account the risk level of all repositories of electronic PHI.
- The Security Officer shall periodically review products and software that been certified or validated by the National Institute of Standards and Technology as being secure, and determine whether any such products should be adopted and implemented.

Document Retention

The Security Officer shall forward a copy of the evaluation to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
FACILITY ACCESS CONTROLS

Section: Security  Subsection: Physical Safeguards  Effective Date: June 1, 2008  Last Reviewed On: September 23, 2013

POLICY

The Plan shall maintain controls that limit physical access to the Plan’s electronic information systems and/or the Facilities in which the systems are housed. Only authorized personnel shall have physical access to such systems and/or Facilities.

PROCEDURE

Contingency Operations [Addressable]

The Security Officer shall establish and develop a plan that allows (and limit) access to the Facility and the Location to only those persons designated by the Security Officer to support the restoration of lost data and/or to implement emergency mode operations.

Facility Security Plan [Addressable]

The Security Officer shall coordinate the preparation of a Facility Security Plan, which shall document the physical measures taken by the Plan to prevent (i) unauthorized access to the Facility and (ii) tampering or theft of its information systems containing the Plan’s electronic PHI. Buildings containing electronic PHI shall have either logged magnetic card access or monitored access control by a receptionist. Additionally, if electronic PHI is left unattended, the door to that area shall be locked. After hours, a site security guard shall monitor all access to all buildings. The security guard will be on-site 24 hours a day, 7 days a week and will accommodate any authorized request for contingency or emergency access to electronic PHI. Facility maintenance records regarding security and access issues shall be maintained by the Security Officer.

Access Control and Validation Procedures [Addressable]

The following procedures control and validate a person’s access to the Facility and/or the Location based on their role or function:

- Facility
  - Entry points to the Facility are open to the public during normal business hours. During those hours, the entry points are manned by personnel who are able to distinguish employees from visitors.
  - All employees regularly scheduled to work at the Facility are provided with ID badges and/or Facility Access Cards.
- All visitors to the Facility are required to present identification and sign a Visitor Log that records the time of arrival and departure.

- **Location**
  - The Location is locked 24 hours per day. Access card readers are located at each of the entry points to the Location. Access is available only through a Special Access Card.
  
  - Employees and visitors who require physical access to the Location must obtain an Special Access Card or must be escorted by an employee with a Special Access Card. The Security Officer shall decide whether an employee or visitor shall be issued a Special Access Card. The Security Officer shall maintain a Special Access Log recording those persons to whom a Special Access Card is issued.

**Maintenance Records [Addressable]**

Workforce Members shall inform the Security Officer of all physical repairs or maintenance that may affect the security of the Facility or the Location. The Security Officer shall document this information in a Maintenance Log.

The Security Officer shall document in the Maintenance Log all maintenance performed on the information system hardware that stores or has access to the Plan’s *electronic PHI*.

**Document Retention**

The Security Officer shall forward a copy of the Facility Access Plan to the Privacy Officer, who shall maintain a copy in a file specifically designed for that purpose. The file shall be subject to the document retention provisions of these HIPAA Policies and Procedures.

No less than annually, the Security Officer shall forward a copy of the Visitor Log, the Special Access Log, and the Maintenance Log to the Privacy Officer, who shall maintain a copy in files specifically designed for that purpose. The files shall be subject to the document retention provisions of these HIPAA Policies and Procedures.
<table>
<thead>
<tr>
<th>Name of Visitor:</th>
<th>Purpose of Visit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time In:</td>
<td>Checked in by (initials):</td>
</tr>
<tr>
<td>Date/Time Out:</td>
<td>Checked out by (initials):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Visitor:</th>
<th>Purpose of Visit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time In:</td>
<td>Checked in by (initials):</td>
</tr>
<tr>
<td>Date/Time Out:</td>
<td>Checked out by (initials):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Visitor:</th>
<th>Purpose of Visit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time In:</td>
<td>Checked in by (initials):</td>
</tr>
<tr>
<td>Date/Time Out:</td>
<td>Checked out by (initials):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Visitor:</th>
<th>Purpose of Visit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time In:</td>
<td>Checked in by (initials):</td>
</tr>
<tr>
<td>Date/Time Out:</td>
<td>Checked out by (initials):</td>
</tr>
</tbody>
</table>
## FORM: SPECIAL ACCESS LOG

Name (person to whom Special Access Card is issued):

Check One: ☐ Employee  ☐ Visitor

* * *

Date and Time Issued: _________________________________

Reason for Issuing:

Initials of Security Officer issuing Special Access Card:

* * *

Date and Time Revoked: _______________________________

Reason for Revoking:

Name (person to whom Special Access Card is issued):

Check One: ☐ Employee  ☐ Visitor

* * *

Date and Time Issued: _________________________________

Reason for Issuing:

Initials of Security Officer issuing Special Access Card:

* * *

Date and Time Revoked: _______________________________

Reason for Revoking:
<table>
<thead>
<tr>
<th>Form: Maintenance Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance performed on (check at least one)</td>
</tr>
<tr>
<td>Describe Maintenance:</td>
</tr>
<tr>
<td>Start Date: ________________</td>
</tr>
<tr>
<td>End Date: ________________</td>
</tr>
<tr>
<td>Maintenance performed on (check at least one)</td>
</tr>
<tr>
<td>Describe Maintenance:</td>
</tr>
<tr>
<td>Start Date: ________________</td>
</tr>
<tr>
<td>End Date: ________________</td>
</tr>
<tr>
<td>Maintenance performed on (check at least one)</td>
</tr>
<tr>
<td>Describe Maintenance:</td>
</tr>
<tr>
<td>Start Date: ________________</td>
</tr>
<tr>
<td>End Date: ________________</td>
</tr>
<tr>
<td>Maintenance performed on (check at least one)</td>
</tr>
<tr>
<td>Describe Maintenance:</td>
</tr>
<tr>
<td>Start Date: ________________</td>
</tr>
<tr>
<td>End Date: ________________</td>
</tr>
</tbody>
</table>
WORKSTATION USE AND SECURITY

Section: Security
Subsection: Physical Safeguards
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

Workstations that contain or have access to electronic PHI shall be used only by authorized persons and only in a manner that protects the security of the electronic PHI.

PROCEDURE

Except as described in the Facility Access Controls Policy or below, access to the Plan’s electronic PHI is generally managed through technical means (username and password) and not physical means. However, the following physical security measures shall be observed:

- If a workstation may be used to access PHI, the screen of the workstation shall be oriented away from traffic patterns used by unauthorized persons, so that unauthorized persons generally will not be able to observe any PHI without alerting the suspicion of others.

- Except for workstations in the Location or in a locked room, workstations will be generally observable by more than one employee.

- Workforce Members shall question any unauthorized person using another’s workstation or shall report such use to the Security Officer.

- Workforce Members shall question any unauthorized person that appears to be viewing PHI on a workstation or shall report such use to the Security Officer.

- Workforce Members, independent contractors and consultants who use the Plan’s information systems infrastructure should have no expectation of privacy. To appropriately manage its information system assets, the Plan may log, review, or monitor any data (regardless of whether it constitutes electronic PHI) stored or transmitted on its information systems.

- The Plan may limit or remove access to its information system infrastructure, in its sole discretion. This includes, but is not limited to, restricting or removing user access accounts, limiting or restricting access to secured areas. The Security Officer shall make appropriate determinations on a case-by-case basis as necessary to preserve the integrity, confidentiality, and availability of its information system infrastructure and data that contain electronic PHI.

- Each workstation that is used to access, transmit, receive or store electronic PHI must comply with each of the following measures. If any of these measures are not supported by the workstation operating system or system architecture, one of the following steps must be taken: (i) the server, desktop computer system, or wireless computer system must be upgraded to support the security measures referenced below; (ii) an alternative security
measure must be implemented and documented, or (iii) the workstation must not be used to send, receive, or store electronic PHI.

**Server Security Requirements**

- The Security Officer shall ensure that all servers used to access, transmit, receive or store electronic PHI are appropriately secured in accordance with this Policy.
- Servers shall be located in a physically secure environment.
- The system administrator or root account shall be password protected.
- A User Identification and password authentication mechanism shall be implemented to control user access to the system.
- A security patch and update procedure shall be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- Servers shall be located on a secure network with firewall protection. If for any reason the server must be maintained on a network that is not secure, an intrusion detection system must be implemented on the server to detect changes in operating and file system integrity.
- All unused or unnecessary services shall be disabled.

**Desktop System Security Requirements**

- The Security Officer shall ensure that each desktop system used to access, transmit, receive or store electronic PHI is appropriately secured in accordance with this Policy.
- The system administrator or root account shall be password protected.
- A user identification and password authentication mechanism shall be implemented to control user access to the system.
- A security patch and update procedure shall be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- A virus detection system shall be implemented including a procedure to ensure that the virus detection software is maintained and up to date.
- All unused or unnecessary services shall be disabled.
- Desktop systems that are located in open, common, or otherwise insecure areas shall also implement the following measures: (i) an inactivity timer or automatic logoff mechanism must be implemented, or (ii) the workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.
Mobile Systems Security Policy

- The Security Officer shall ensure that all mobile systems used by employees to access, transmit, receive or store electronic PHI are appropriately secured in accordance with this Policy.
- The system administrator or root account shall be password protected.
- A user identification and password authentication mechanism shall be implemented to control user access to the system. All mobile devices and laptops shall use a boot password to ensure that the system is only accessible to authorized users.
- A security patch and update procedure shall be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- A virus detection system shall be implemented including a procedure to ensure that the virus detection software is maintained and up-to-date.
- All unused or unnecessary services shall be disabled.
- Mobile stations that are located or used in open, common, or otherwise insecure areas shall also implement the following measures: (i) a theft deterrent device such as a laptop locking cable must be utilized when the device is unattended; or (ii) an inactivity timer or automatic logoff mechanism must be implemented.
- Reasonable safeguards shall be in place to prohibit unauthorized entities from viewing confidential information such as logins, passwords, or electronic PHI.
- Personal Digital Assistants (“PDAs”) and other handheld mobile devices shall not be used for long-term storage of electronic PHI. Electronic PHI stored on hand held mobile devices must be purged as soon as it is no longer needed on that device, with a storage time not to exceed thirty (30) days.
- Each mobile system that is used to access, transmit, receive, or store electronic PHI shall comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.
POLICY

The Plan manages the receipt, removal and movement of hardware and electronic media that contain electronic PHI.

PROCEDURE

The Security Officer shall create, maintain, and update an inventory of the Plan’s hardware and electronic media containing electronic PHI. This procedure applies, but is not limited to, the use of hard drives, storage systems, removable disks, floppy drives, CD-ROMs, memory sticks, and all other forms of removable media and storage devices.

Disposal [Required]

A Privacy Worker disposing of electronic media containing PHI shall clear, purge, or destroy the media consistent with NIST Special Publication 800-88, Guidelines for Media Sanitation, (available at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf) such that the PHI cannot be retrieved.

- If the device or media contains the only copy of electronic PHI that is required or needed, a retrievable copy of the electronic PHI must be made prior to disposal.

- If the device or media contains electronic PHI that is not needed or required, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat shall not be sufficient as it does not overwrite the data.

- The Privacy Worker shall inform the Security Officer of the disposal.

- The Security Officer shall note the disposal in the Security Inventory.

Media Re-use [Required]

This procedure applies when electronic media containing electronic PHI will be re-used to store new information, if the new information will be accessible to persons who would not have had access to the electronic PHI.

- Prior to any re-use of electronic media, a Privacy Worker shall clear or purge the media of electronic PHI, consistent with NIST Special Publication 800-88, Guidelines for Media Sanitation, (available at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf) such that the electronic PHI cannot be retrieved.
• If the device or media contains the only copy of the *electronic PHI* that is required or needed, a retrievable copy of the *electronic PHI* shall be made prior to reuse.

• If the device or media contains *electronic PHI* that is not required or needed, and is not a unique copy, a data destruction tool shall be used to destroy the data on the device or media prior to reuse. A typical reformat shall not be sufficient as it does not overwrite the data.

• If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secure environment, the use of a data destruction tool between uses is not necessary.

• The Privacy Worker shall inform the Security Officer of the clearing or purging before re-using the media and before making the media available to others for re-use.

• The Security Officer shall note clearing or purging in the Security Inventory.

**Accountability, Data Backup, and Data Storage [Addressable]**

**Hardware**

• A Workforce Member bringing hardware into the Facility shall inform the Security Officer. If the hardware will contain *electronic PHI*, the Security Officer will record the hardware on the Security Inventory.

• If hardware contains *electronic PHI*, a Workforce Member shall inform the Security Officer prior to moving the hardware. The Security Officer shall determine whether it is necessary to create a retrievable, exact copy of the *electronic PHI* contained on the hardware prior to moving the hardware. If so, the Security Officer will ensure that such a copy is created. The Security Officer will record the movement of the hardware on the Security Inventory.

**Electronic Media**

• A Privacy Worker using *electronic media* to store *electronic PHI* shall inform the Security Officer. The Security Officer shall record the *electronic media* on the Security Inventory.

• If *electronic media* contains *electronic PHI*, a Workforce Member shall inform the Security Officer prior to moving the media. The Security Officer shall determine whether it is necessary to create a retrievable, exact copy of the *electronic PHI* on the media prior to moving the media. If so, the Security Officer shall ensure that such a copy is created. The Security Officer shall record the movement of the hardware on the Security Inventory.

**Data Backup and Storage**

• The Security Officer shall establish and maintain a data backup plan. Among other things, the data backup plan shall provide for criteria as to when a retrievable, exact copy of *electronic PHI* is required before movement of equipment.
TECHNICAL ACCESS CONTROL

Section: Security
Subsection: Technical Safeguards
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

Technical security measures are implemented for the Plan’s electronic information system that maintains electronic PHI to allow access only to those persons or software programs that have been granted access rights.

PROCEDURE

Unique User Identification [Required]

Privacy Workers who are authorized to access electronic PHI shall be assigned (or shall be required to create) a unique User ID. The Plan’s information system will use the User ID to identify and track user identity.

The User ID will allow the Privacy Worker to access electronic PHI only to the extent that access privileges have been authorized under the Administrative Safeguards in these HIPAA Policies and Procedures.

Privacy Workers shall not allow anyone else to use their unique User ID and Privacy Workers shall ensure that their User ID and secure password are not documented, written or otherwise exposed in an insecure manner.

If a Privacy Worker has reason to believe that either their User ID or password has, in any way, been compromised, then he or she shall report the security incident to the Security Officer.

Emergency Access Procedure [Required]

In emergency situations, the Security Officer has the power to authorize temporary access to electronic PHI. The relevant procedures are described in the Plan’s contingency plan.

Automatic Logoff [Addressable]

The Security Officer shall ensure that all servers, workstations, or other computer systems that access, transmit, receive, or store electronic PHI will employ inactivity timers or automatic logoff mechanisms (e.g. a password protected screensaver that blacks out screen activity). Such systems shall terminate a user session after a maximum of, but not limited to, fifteen (15) minutes of inactivity.

All applications and databases that use electronic PHI shall employ inactivity timers or automatic session logoff mechanisms. Such software must automatically terminate user sessions
after a maximum of, but not limited to, fifteen (15) minutes of inactivity.

All users shall shut down or logoff whenever they leave unattended any computer system, any application or database that accesses, transmits, receives or stores electronic PHI.

**Termination of Access**

Upon termination of a Workforce Member’s employment, the Security Officer shall complete a Termination of Access Checklist and shall terminate the Workforce Member’s access to all electronic PHI, the Plan’s information systems, and buildings housing Plan information (electronic or otherwise). Access may be terminated earlier if circumstances so require.

When a Workforce Member no longer needs access to electronic PHI, the Security Officer shall complete a Termination of Access Checklist and shall terminate the Workforce Member’s access to all electronic PHI.

**Encryption and Decryption [Addressable]**

The Security Officer shall develop and implement procedures to encrypt highly critical or sensitive electronic PHI.

The Security Officer shall determine when electronic PHI will need to be encrypted as a transmission control and integrity mechanism.

**Remote Access**

Dial up connections directly into secure networks are considered to be secure connections and do not require a Virtual Private Network (“VPN”) connection. This assumes that the remote user is using a secure Public Switched Telephone Network (“PSTN”) connection.

Authentication and encryption mechanisms are required for all remote access sessions to networks containing electronic PHI via an Internet Service Provider (an “ISP”). Examples of acceptable mechanisms include, but are not limited to, VPN clients, authenticated SSL web sessions, and secured Citrix client access.

Mechanisms to bypass authorized remote access mechanism are strictly prohibited on any computer network that contains electronic PHI. Examples of such prohibited applications: PCAnywhere, GoToMyPC.com

Remote access systems must employ some kind of process to erase cache and other session information at the end of a remote user session.

Remote access systems must have virus detection and protection software.

Any encryption process must employ a minimum of 128-bit encryption.

VPN split-tunneling is prohibited for remote access users.
AUDIT CONTROLS

Section: Security
Subsection: Technical Safeguards
Effective Date: June 1, 2008
Last Reviewed On: September 23, 2013

POLICY

The Plan shall use appropriate hardware and software to record activity in information systems that contain or use electronic PHI. The Security Officer shall examine the record periodically to confirm the Plan’s compliance with these security policies and procedures.

PROCEDURE

The Security Officer shall ensure—through the purchase and use of appropriate products or services—that the Plan has the ability to record activity in the Plan’s information systems that contain or use electronic PHI.

Audit Control Mechanisms

The Security Officer shall determine which information systems contain electronic PHI and implement a mechanism which logs and stores system activity.

The information system audit log must include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.

Audit Control and Review Plan

An audit control and review plan shall be developed by the Security Officer. If the Plan’s electronic PHI inventory changes, its audit control and review plan shall be reevaluated: The Plan must include the:

- system applications to be logged;
- information to be logged for each system;
- log-in reports for each system; and
- procedures to review all audit logs and activity reports.

The products and services shall alert the Security Officer to any attempted, suspected, or actual unauthorized access to electronic PHI. Alternatively, the Security Officer shall examine the records referenced above no less than monthly in order to determine whether there has been any access to electronic PHI other than as permitted by these security policies and procedures. Based on the alerts or examinations, the Security Officer may suggest revisions to these security policies and procedures.
## INTEGRITY

<table>
<thead>
<tr>
<th>Section: Security</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
</table>

### POLICY

*Electronic PHI* in the Plan’s information system is protected from improper alteration and destruction.

### PROCEDURE

Electronic mechanisms including, but not limited to, User IDs, password protection for workstations and applications, audit activity logs, and encryption of *electronic PHI* shall be utilized to ensure that *electronic PHI* is not altered or destroyed in an unauthorized manner.

The following electronic mechanisms may be used to corroborate that *electronic PHI* has not been improperly altered or destroyed: error correcting memory, built-in data authentication, digital signatures, and check sum technology.
### PERSON OR ENTITY AUTHENTICATION

<table>
<thead>
<tr>
<th>Section: Security</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
</table>

#### POLICY

The Plan’s information system verifies that a person or entity seeking access to *electronic PHI* is the one claimed.

#### PROCEDURE

As described elsewhere in these security policies and procedures:

- A unique User ID shall be assigned to Workforce Members who are authorized to access *electronic PHI*.

- Workforce Members shall be required to follow the portions of these HIPAA Policies and Procedures concerning passwords in order to safeguard their User IDs.

- Workforce Members shall not disclose their User ID or password to other users, except as may be specifically permitted by these HIPAA Policies and Procedures.

- Workforce Members shall not misrepresent themselves by using another person’s User ID, password, smart card, or other authentication information.

Before gaining access to *electronic PHI*, a user shall be required to represent that he or she is the person to whom the applicable User ID has been assigned.

The authentication system utilized by the Plan shall be periodically tested and upgraded when upgrades are available. The Security Officer shall document the testing results and upgrades for purposes of verifying that the testing was performed and/or the upgrades were applied.
## TRANSMISSION SECURITY

<table>
<thead>
<tr>
<th>Section: Security</th>
<th>Effective Date: June 1, 2008</th>
</tr>
</thead>
</table>

### POLICY

The Plan uses technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

### PROCEDURE

In conjunction with the Risk Analysis Policy, the Security Officer shall identify the manner in which electronic PHI is electronically transmitted. (For example, some electronic PHI may be transmitted over a dial-up line while other electronic PHI may be transmitted over the internet.) The Security Officer shall determine whether the risk of a given type of transmission being improperly accessed is sufficient to warrant integrity controls or encryption.

#### Integrity controls [Addressable]

Prior to transmitting electronic PHI from the Plan to an outside network, the receiving person or entity must be authenticated.

All transmissions of electronic PHI from the Plan to an outside network should only include the minimum amount of PHI.

#### Encryption [Addressable]

- All transmissions of electronic PHI from the Plan to a network outside of the Plan’s network must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing electronic PHI must be encrypted before transmission.

- When transmitting electronic PHI via removable media, including but not limited to floppy disks, CD ROM, memory cards, magnetic tape and removable hard drives, the sending party must: (i) use an encryption mechanism to protect against unauthorized access or modification, (ii) authenticate the person or entity requesting the electronic PHI, and (iii) send the minimum amount of electronic PHI required by the receiving person or entity.

- If using removable media for the purpose of system backups and disaster recovery and the removable media is stored and transported in a secured environment, no additional security mechanisms are required.

- The transmission of electronic PHI over a wireless network within the domain of Trinity University is permitted if the following conditions are met: (i) the local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized, and (ii) the local wireless network is utilizing an encryption mechanism for all transmissions over the wireless network.
If transmitting *electronic PHI* over a wireless network that is not utilizing an authentication and encryption mechanism, the *electronic PHI* must be encrypted before transmission.

The authentication and encryption security mechanisms implemented on wireless networks within the Trinity University domain are only effective within Trinity University’s network. When transmitting outside of this wireless network, additional and appropriate security measures must be implemented in accordance with this policy.

When transmitting *electronic PHI* over an electronic network between the Plan and a Trinity University entity, the *electronic PHI* must be password protected or encrypted before transmission.

All transmissions of *electronic PHI* from the Trinity University domain into the Plan’s network must utilize an encryption mechanism.

All transmissions of *electronic PHI* from the Plan into the Trinity University domain must utilize a mechanism to encrypt or password-protect the *electronic PHI*.

**Additional Requirements**

All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

When transmitting *electronic PHI* electronically, regardless of the transmission system being used, Workforce Members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the *electronic PHI* requested.

If the *electronic PHI* being transmitted is not to be used for treatment, payment or health care operations, only the minimum required amount of *electronic PHI* should be transmitted.