******

**Human Resources Operating Procedure No. 123**

**HIPAA Privacy and Security**

**Trinity Health Corporation Welfare Benefit Plan**

**Trinity Health Corporation Retiree Benefit Plan (Grandfathered)**

**Integrity & Compliance Policy No. 01 Integrity & Compliance Program**

EFFECTIVE DATE*:* January 1,2017

Original Effective Date: April 14, 2003

PROCEDURE TITLE:

***Business Associate Agreements***

***To be reviewed every three years by:***

***Trinity Health Corporation Welfare Benefit Plan Privacy Official***

**REVIEW BY: January 1, 2020**

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This Procedure is in furtherance of the Trinity Health Corporation Integrity & Compliance Program as set forth in Trinity Health Corporation Integrity & Compliance Policy No. 01.

**PURPOSE**

The purpose of this Procedure is to protect, through the execution and enforcement of written agreements, the privacy and confidentiality of PHI that comes into the possession and custody of the Plan and ensure compliance with respect to written Business Associate Agreement requirement in HIPAA. If the regulations under HIPAA are changed by HHS the Plan will follow the revised regulations.

**PROCEDURES**

***1. Identification, Compilation and Maintenance of Business Associate Relationships***

The Plan’s Privacy Official is responsible for:

a. Developing a process to identify all parties who are Business Associates of the Plan. This Procedure does not apply to every arrangement or contract between the Plan or Plan Sponsor and another person or organization. It only applies to a contract where the other person or organization is acting as a Business Associate. Any arrangement with a person or organization serving as a Business Associate but where there is no underlying written contract must also be subject to a Business Associate Agreement.

i. All Workforce Members and other Plan Sponsor employees must forward to the Plan’s Privacy Official or its delegate all proposed agreements between the Plan or Plan Sponsor and a Business Associate where a Business Associate Agreement is necessary. If a Workforce Member or other Plan Sponsor employee is uncertain whether the Plan will provide access to PHI, he or she is instructed to forward the agreement to the Privacy Official or his or her delegate for review.

ii. The Privacy Official or his or her delegate, with the assistance of legal counsel as appropriate, will review each agreement between the Plan or Plan Sponsor and each outside vendor to determine whether a Business Associate Agreement with each outside vendor providing services to or on behalf of the Plan is required.

b. Ensuring the Plan enters into a written Business Associate Agreement with a Business Associate prior to allowing the Business Associate to access, Use, Disclose, create, maintain or transmit PHI on behalf of the Plan.

c. Coordinating the execution of Business Associate Agreements.

d. Compiling an inventory list of executed Business Associate Agreements.

e. Updating the Business Associate Agreement inventory list as new Business Associate Agreements are executed or replaced.

f. Reviewing the Business Associate Agreement inventory list at least annually to assess whether the list is being properly maintained, accurate and complete.

g. Determining where the Business Associate Agreements will be stored/maintained (e.g., at a central location, within applicable departments, etc.).

***2. Business Associate Agreements***

a. A Business Associate Agreement must be in writing and must incorporate the required provisions of 45 CFR § 164.504(e). The Plan’s Privacy Official or his or her delegate, with the assistance of legal counsel, will prepare a standard Business Associate Agreement for the Plan that satisfies these requirements.

B. If a Business Associate Agreement is required with respect to an agreement, contract or arrangement, the Plan’s standard Business Associate Agreement shall be used. Any modifications must be approved by the Plan’s Privacy Official or his or her delegate, with the assistance of legal counsel as appropriate. The Privacy Official and his or her delegate shall also be notified upon termination of the relationship.

# DEFINITIONS

The following are definitions of key terms used in this Procedure. Any terms used in this Procedure, but not otherwise defined herein, shall have the meaning set forth in the HIPAA regulations, 45 CFR §§ 160.103, 164.103, 164.304, 164.402 and 164.501.

**Business Associate means**, with respect to a Covered Entity, a person or organization that:

1. Creates, receives, maintains, or transmits PHI for a function or activity on behalf of a Covered Entity other than in the capacity of a member of the Covered Entity’s Workforce; or

2. Provides, other than in the capacity of a member of the Covered Entity’s Workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Covered Entity, where the provision of the service involves the Disclosure of PHI from the Covered Entity, or from another Business Associate of the Covered Entity, to the person.

However, a person or organization is not a Business Associate if it is:

3. A health care provider (e.g., hospital medical staff), with respect to Disclosures by a Covered Entity to the health care providing concerning the treatment of an individual; or

4.. A plan sponsor with respect to Disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent the requirements of 45 CFR § 164.504(f) of HIPAA apply and are met.

The following are definitions of key terms used in this Procedure. Any terms used in this Procedure but not otherwise defined herein, shall have the meaning set forth in the HIPAA Administrative Simplification Regulations, 45 CFR §§ 160.103, 164.103, 164.304, 164.402 and 164.501.

**Business Associate Agreement means** a written contract or other written agreement or arrangement between a Covered Entity and a Business Associate that allows the Business Associate to create, receive, maintain or transmit PHI on behalf of the Covered Entity.

**Covered Entity means** (a) a health plan, (b) a healthcare clearinghouse, or (c) a health care provider who transmits any health information in an electronic form in connection with a transaction covered under 45 CFR Subtitle A, Subchapter C, Parts, 160, 162 and 164.

**Disclosure (or Disclose) means**, with respect to PHI, the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

**HHS means** the U.S. Department of Health and Human Services.

**HIPAA means** the Privacy Standards of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), 42 U.S.C. § 1320d, et. seq., and the regulations issued thereunder, 45 CFR Parts 160 and 164, as amended from time to time.

**Individual** **means** the person who is the subject of PHI and who is also a participant or former participant in the Plan or a covered spouse, dependent or beneficiary under the Plan.

**Individually Identifiable Health Information means** information that is a subset of health information, including demographic information collected from an Individual, and that:

1. Is created or received by a health care provider, health plan, employer, or health care clearing house; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and

3. Identifies the Individual or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

**Plan means** the Trinity Health Corporation Welfare Benefit Plan (“Welfare Plan”) and the Trinity Health Corporation Retiree Benefit Plan (Grandfathered) (“Retiree Plan”), with respect to the benefit programs thereunder that constitute “health plans,” as defined in 45 CFR § 160.103. For the Welfare Plan, the benefit programs that constitute health plans are the medical/prescription drug, dental, vision, employee assistance, flexible healthcare spending account and healthcare reimbursement account program components of the Plan. For the Retiree Plan, the benefit programs that constitute health plans are the medical/prescription drug, dental, vision and healthcare reimbursement account program components of the Plan. The Welfare Plan and the Retiree Plan are each a Covered Entity. Whenever reference is made to the Plan’s action, the activities of the Plan Sponsor on behalf of the Plan shall be treated as the action of the Plan.

**Plan Sponsor** **means** the “plan sponsor” as defined in section 3(16)(B) of ERISA, 29 U.S.C. § 1002(16)(B) and means Trinity Health Corporation and, except where context indicates otherwise, employees and agents of Trinity Health Corporation and the other participating employers in the Plan who are responsible for Plan administration functions.

**Privacy Official means** the person designated by the Plan or Plan Sponsor to oversee and administer the Plan’s compliance with these Procedures and HIPAA.

**Protected Health Information or PHI means** Individually Identifiable Health Information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes Individually Identifiable Health Information: (a) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (b) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (c) in employment records held by a the Plan Sponsor or a Covered Entity in its role as employer; and (d) regarding a person who has been deceased for more than 50 years.

**Use (or Uses) means**, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

**Workforce or Workforce Member** **means** employees and other persons whose conduct, in the performance of work for the Plan, is under the direct control of the Plan or Plan Sponsor or one of its affiliated entities on behalf of the Plan, whether or not they are paid by the Plan or Plan Sponsor or one of its affiliated entities. The Workforce Members are described in Section 2.a.i. of this Procedure.

**RELATED PROCEDURES AND OTHER MATERIALS**

* Human Resources Operating Procedure No. 120 (Use or Disclosure of Protected Health Information)
* Enterprise Information Security Procedures
* Standard Business Associate Agreement
* List of Business Associates
* List of Business Associate Agreements

**APPROVALS**

**Initial Approval: 04/14/2003**

**Subsequent Review/Revisions: December 20, 2016**

Omnibus BAA-When TH Welfare Benefit Plan is Covered Entity

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) is entered into by and between the [Trinity Health Corporation Welfare Benefit Plan] [Trinity Health Retiree Medical Plan (Grandfathered)] (and all of the group health benefit plans thereunder) (the “Plan” and the “Covered Entity”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Business Associate”) and applies to all services provided to or on behalf of the Covered Entity and relationships between Covered Entity and Business Associate.

1. HIPAA and HITECH Dominance. In the event of a conflict or inconsistency between the terms of any other agreement between the parties (or between the Plan Sponsor, as defined by HIPAA) on behalf of the Plan and Business Associate) and this language, this BAA language controls with respect to the subject matter herein. This language is required by the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act (found in Title XIII of the American Recovery and Reinvestment Act of 2009) (“HIPAA” and “HITECH”). The parties acknowledge and agree that, beginning with the effective dates under HIPAA and HITECH, Business Associate will comply with its obligations under this BAA and with all obligations of a business associate under HIPAA, HITECH and any implementing regulations, as they exist at the time this BAA is executed and as they are amended from time to time, for so long as this BAA is in place. (Collectively, HIPAA and HITECH are referred to herein as “HIPAA”). The terms used but not defined in this BAA have the same meaning as defined by HIPAA unless the context dictates otherwise.
2. HIPAA Applicability and Scope: Business Associate and Subcontractors. For purposes of the obligations under this BAA, the term “subcontractor” means, collectively, all of the Business Associate’s subcontractors as well as each of their downstream entities. Business Associate and its subcontractors are directly subject to and must independently comply with the Business Associate provisions of HIPAA irrespective of the provisions contained in this BAA.

1. Protected Health Information. Any Protected Health Information (“PHI”) as defined by HIPAA that, on behalf of Covered Entity, was collected, created, received, maintained by or transmitted to or from Covered Entity is PHI. For purposes of these obligations PHI means all PHI in Business Associate’s possession or under its control (e.g., employees, workforce members, subcontractors and their downstream entities, and subcontractors) and all PHI collected, created, received, maintained or transmitted by Business Associate or its subcontractors on or after the effective date of this HIPAA language.
2. Confidential Information. Confidential Information means and includes (a) any and all information related to Individuals who are or were covered under the Plan; (b) any and all information about Covered Entity that is not known to the general public; (c) non-public information that belongs or relates to third parties to whom Covered Entity has an obligation of confidentiality, including software vendors; and (d) non-public information about the Plan Sponsor’s or its affiliated entities’ Covered Entity’s employees or business associates.
3. Employees, Subcontractors and Disciplinary Action
   1. Acts / Omissions. Business Associate will be responsible for all actions and/or omissions by its employees and/or subcontractor’s employees and is liable to third parties and Covered Entity for any violation of an Individual’s privacy or security by any person granted access or receiving data through Business Associate. For purposes of this BAA, the Business Associate’s employees include its workforce members.
   2. Employees. Business Associate agrees to instruct its employees regarding the confidentiality, privacy and security of PHI and the Business Associate’s obligations under this BAA. Business Associate shall not disclose to its employees or permit them to access, view, obtain, copy, review or use any PHI that is not necessary to their services to Covered Entity. Business Associate agrees to maintain strict performance standards, including disciplinary actions, with respect to wrongful access to, copying, viewing, misuse or disclosure of PHI.
   3. Workforce Members and Downstream Entities. Business Associate shall ensure its permitted workforce member(s) and subcontractor(s) (if subcontractors are permitted) that collect, create, receive, maintain, or transmit PHI on behalf of the Covered Entity are advised in writing of Business Associate’s obligations with respect to PHI. Business Associate shall require that the permitted subcontractor(s) agree in writing to the same permissible uses and disclosures of PHI and to the same restrictions, conditions and obligations that apply to the Business Associate. Business Associate agrees to make a list of such subcontractors available to Covered Entity upon request.
   4. Administrative and Disciplinary Action. Business Associate will take appropriate administrative and disciplinary action with respect to its employee or subcontractor if a privacy and/or security violation is substantiated.
4. Permissible Uses of PHI.
5. Using and Disclosing PHI. Business Associate is a person or an organization, other than a member of a Covered Entity’s workforce, that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involves the use or disclosure of PHI. Business Associate may use or disclose PHI as permitted by this BAA or as required by law.

Furthermore, the Business Associate may only use or disclose PHI to the extent that the Covered Entity is permitted to use and disclose PHI and, only if, the Covered Entity has delegated that use or disclosure to the Business Associate.

1. Business Associate’s Internal Management Uses of PHI. Business Associate may use PHI for internal management and administration of Business Associate, but only in connection with the direct performance by Business Associate through its employees of services for Covered Entity pursuant to this BAA.
2. Minimum Necessary. Business Associate is permitted to access, use, request, disclose and/or store only the minimum necessary PHI to the extent required to perform its duties under this BAA.
3. Handling PHI. Business Associate agrees to promptly return or destroy any PHI that is erroneously shared or delivered to Business Associate.
4. Data Aggregation. Business Associate is permitted to use PHI for data aggregation for the health care operations of Covered Entity and only as required by a written contract between Business Associate and Covered Entity or upon written request of Covered Entity. Data aggregation means combining Covered Entity’s PHI with another unrelated covered entity’s PHI for any purpose.
5. De-Identified – Business Associate Use for Own Purposes. Business Associate agrees not to sell (i.e., receive any direct or indirect remuneration) or use any PHI, de-identified PHI or data that identifies the Covered Entity for its own purposes or for the benefit of its other customers, without Covered Entity’s prior written consent. Furthermore, in cases where the Business Associate requests consent to de-identify PHI, the Business Associate shall specify to the Covered Entity the manner in which the Business Associate will de-identify the information.
6. No Indirect Sale of PHI. Business Associate has not given Covered Entity a discount or reduction in pricing in exchange for purposes other than services to or on behalf of Covered Entity.

8. Disclosure of PHI to Plan Sponsor.

a. Business Associate may disclose Summary Health Information (as defined by HIPAA) to the Plan Sponsor (as defined by HIPAA) provided that a written request from the Plan Sponsor specifies a HIPAA permitted purpose for the receipt and use of the Summary Health Information and the Plan approves the requested disclosure in writing.

b. Business Associate will not disclose PHI, other than Summary Health Information, to the Plan Sponsor, except upon written request of the Plan and certification by the Plan that the disclosure is permitted by the Plan documents.

c. Business Associate may disclose or provide access to PHI, other than Summary Health Information, to carry out the plan administration functions that the Plan Sponsor performs for the Plan, but only to those employees or other persons (including third parties) identified in a written request approved by both the Plan and Plan Sponsor.

9. Disclosures to and Agreements by Third Parties**.** Upon Plan's written request, Business Associate will provide PHI to certain Plan designated third parties who assist in administering the Plan and who are authorized by the Plan to receive such information (“Designated Third Parties”). Such Designated Third Parties may include, but are not limited to, third-party administrators, consultants, brokers, auditors, successor administrators or insurers, and stop-loss carriers. Plan agrees to enter into and maintain a Business Associate Agreement with Designated Third Parties to whom it directs Business Associate to disclose PHI, when such an agreement is required by law.

1. Safeguards, Reporting, Mitigation and Standard Transactions
2. Safeguards and Security. Business Associate agrees to implement reasonable administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of all PHI and to inhibit both the use or disclosure of PHI other than as permitted by this BAA and security incidents. Business Associate agrees to implement reasonable electronic security practices for Covered Entity PHI which is transmitted, stored, collected, created, received, maintained or used in electronic form to inhibit both the use or disclosure of PHI other than as permitted by this BAA and security incidents. Business Associate also shall require its permitted subcontractor(s) to agree in writing to implement reasonable administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of all Covered Entity’s PHI and to inhibit both the use or disclosure of PHI other than as permitted by this BAA and security incidents. Business Associate agrees to secure PHI through the use of encryption and/or destruction as required by Covered Entity’s procedure for its internal information systems, including on portable devices and removable media. The Business Associate agrees to encrypt PHI transmitted by the Business Associate to the Covered Entity over a public network.

2. Reporting of Actual or Suspected Violations.

a. Notification. Business Associate shall notify the designated Privacy Official and/or Security Official of Covered Entity in writing within five (5) business days after discovery of any actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI not permitted by this BAA or any other agreement between the parties (or between the Plan Sponsor on behalf of the Plan and Business Associate), if applicable. Business Associate shall take prompt corrective action to cure any such deficiencies and actions pertaining to such unauthorized use or disclosure of PHI or ePHI not permitted by this BAA, made by its employees and/or subcontractors, and will cooperate with Covered Entity in the investigation of these incidents. Furthermore, upon request of the Covered Entity, Business Associate will report, in summary form, any unsuccessful security incident of which Business Associate becomes aware. If the definition of “security incident” in the HIPAA regulation is modified to remove the requirement for reporting “unsuccessful” security incidents, this paragraph shall no longer apply as of the effective date of such regulation modification.

b. Content - Reporting of Actual or Suspected Violations. Business Associate shall report to the Covered Entity, to the best extent reasonably possible, the identification of each Individual whose PHI or ePHI has been, or is reasonably believed by the Business Associate, to have been accessed, acquired, or disclosed in connection with an actual or suspected breach of privacy, security or HITECH. Business Associate shall also provide Covered Entity with any other available information that Covered Entity is required to include in a notification to an Individual, as well as any information necessary to complete an assessment of the risk of compromise to the Individual’s PHI. In addition, Business Associate shall provide Covered Entity with continuous updates concerning the details of an actual or suspected breach of privacy or security, including efforts made to mitigate the extent of compromise, if any.

c. Risk Assessment and Investigation. Business Associate shall cooperate with Covered Entity in performing an appropriate risk assessment immediately following the discovery of any unauthorized access, use or disclosure of PHI. In performing a risk assessment, Business Associate and Covered Entity shall consider all factors listed at 45 C.F.R. § 164.402(2)(i)-(iv) in determining the probability that an Individual’s PHI has been compromised.

d. Mitigation. Business Associate agrees to maintain adequate procedures for mitigation in the event of an actual or suspected breach of privacy or security, which require, for example, promptly obtaining reasonable assurances from the unauthorized recipient of PHI that the information will not be further used or disclosed or will be destroyed. Business Associate agrees to cooperate and collaborate with the Covered Entity in mitigating any harmful effect that is known to Business Associate, including known to its employees/ subcontractors, of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA. Business Associate also agrees to be responsible for any mitigation or compliance costs related to a breach of privacy or security caused by the Business Associate or its subcontractors.

e. Notification to Individual. Upon receiving notice of an actual or suspected breach of privacy or security from Business Associate, Covered Entity, in its sole discretion, will determine whether it or Business Associate will notify Individuals of any breach of unsecured PHI as necessary or required by HITECH. Business Associate shall cooperate with Covered Entity as necessary to provide such notification to impacted Individuals.

f. Notification to Media. For a breach of PHI involving more than 500 Individuals, Covered Entity will notify the media as required by HITECH, 45 C.F.R. § 164.406, unless Covered Entity expressly permits Business Associate to do so on its behalf. At no time is Business Associate to contact or speak directly with the media without the prior authorization of Covered Entity. Business Associate shall cooperate with Covered Entity as necessary to provide such notification to the media.

3. Standard Transactions. If the Business Associate is conducting all or any part of a Standard Transaction (as defined in HIPAA), electronically, for, or on behalf of the Plan, the Business Associate will comply with each applicable requirement for Standard Transactions.

1. Confidentiality and Pattern of Activity.
2. Confidentiality. All Covered Entity’s Confidential Information is subject to the confidentiality and use and disclosure provisions of federal and state law. Business Associate agrees to maintain the confidentiality of, and to use or disclose, all Confidential Information in accordance with such laws.
3. Notice of Legal Contact. Business Associate shall promptly notify Covered Entity in writing of a disclosure request prior to disclosing Covered Entity PHI if such disclosure is required by law or court order, to the extent as permitted by law.
4. Pattern of Activity. If Business Associate becomes aware of a pattern of activity or practice by Covered Entity that constitutes a material breach or violation of the Covered Entity’s obligations under this BAA, Business Associate will notify Covered Entity of the same.
5. Individual Rights With Respect To PHI.

1. General.Upon request, the Business Associate shall make PHI in its possession or under its control available to the Covered Entity within five (5) business days of a Covered Entity’s request. Business Associate will make PHI available in electronic format upon request by Covered Entity.

2. Notice of Individual Contact. Business Associate shall promptly notify the Privacy Official of Covered Entity if an Individual contacts Business Associate in connection with the Individual’s PHI.

3. Covered Entity’s Obligations.To the extent that the Covered Entity has agreed to any limitations and/or restrictions that affect the Business Associate’s use or disclosure of PHI, the Covered Entity shall so notify the Business Associate of such limitations and/or restrictions, and Business Associate shall comply with the same, including, but not limited to, those limitations listed on the Covered Entity’s Notice of Privacy Practices and/or restrictions agreed upon or required by HIPAA for a specific Individual.

4. Individual Access and Amendment. To the extent that (1) Business Associate is engaged to maintain PHI in a designated record set and (2) Covered Entity agrees to allow Business Associate to facilitate Individual requests for PHI, then the Business Associate agrees to honor Individual rights under HIPAA, including the following:

a. Access to PHI. Within five (5) business days of Covered Entity’s or an Individual’s written request, Business Associate shall provide an Individual who is the subject of the PHI, with access to PHI in Business Associate’s possession, if Business Associate’s information consists of a designated record set, in order for Covered Entity to comply with 45 C.F.R. § 164.524. However, if an Individual requests PHI directly from Business Associate, Business Associate shall notify Covered Entity within five (5) days of the request and if, following such notice to the Covered Entity, the Covered Entity requests the Business Associate not to provide the Individual with access, the Business Associate will honor the Covered Entity’s request. Effective as of the date specified by the U.S. Department of Health and Human Services (“HHS”), in the event that the PHI is in the form of an electronic health record, Business Associate shall provide Covered Entity with access to PHI that enables Covered Entity to comply with 45 C.F.R. § 164.524 and the requirements regarding access to electronic health records.

b. Availability of PHI for Amendment. Within five (5) business days of Covered Entity’s written request, Business Associate shall make PHI contained in a designated record set in Business Associate’s possession available to Covered Entity for amendment and shall incorporate any amendments in accordance with 45 C.F.R. § 164.526.

5. Accounting of Disclosures. Business Associate agrees to document disclosures of PHI and to make available within five (5) business days of Covered Entity’s written request, information to Covered Entity concerning Business Associate’s disclosure of PHI for which Covered Entity needs to provide an Individual with an accounting of disclosures as required by 45 C.F.R. § 164.528.

* + 1. If an Individual requests that Business Associate provide an accounting of disclosures of the Individual’s PHI, Business Associate shall provide the accounting to the Individual and to Covered Entity within five (5) business days of the Individual’s written request.
    2. If an Individual requests that Covered Entity provide an accounting of disclosures of the Individual’s PHI, Covered Entity may direct such Individual to request Business Associate’s accounting of disclosures of the Individual’s PHI directly from Business Associate. In the event Covered Entity directs an Individual to obtain an accounting of disclosures of the Individual’s PHI directly from Business Associate, and the Individual requests such an accounting directly from Business Associate, Business Associate agrees to provide the Individual with an accounting of disclosures of the Individual’s PHI made by Business Associate and to provide a copy of any such account of disclosures to Covered Entity within five (5) business days of the Individual’s written request.
    3. Business Associate will maintain an accounting of such disclosures for at least six (6) years following the date of the disclosure for which an accounting is required (or, beginning on the date specified by HHS, three (3) years for disclosures related to an Electronic Health Record and the exceptions under 45 C.F.R. § 164.528(a)(1)(i) shall not apply).

1. Amendment. Upon enactment of any law, regulation, court decision or relevant government publication and/or interpretive policy affecting the use or disclosure of PHI, Covered Entity, by written notice to Business Associate, may amend or replace this BAA in such manner as Covered Entity determines necessary to comply with same.
2. Access for Audit. Business Associate shall make its internal practices, books and records relating to the use and disclosure of any PHI available to Covered Entity and to other authorized government investigators for purposes of determining Business Associate’s and Covered Entity’s compliance with HIPAA. Business Associate agrees that Covered Entity has the right to audit, investigate, monitor, access, review and report on Business Associate’s use of any Covered Entity’s PHI, with or without advance notice from Covered Entity.
3. Assignment. Business Associate may not assign any rights, nor may it delegate its duties, under this BAA without the express written consent of Covered Entity.
4. Laws. Business Associate will comply with all applicable federal and state security and privacy laws that are more protective of individual privacy and security than HIPAA.
5. Injunctive Relief. Business Associate acknowledges and stipulates that any unauthorized use or disclosure of PHI by Business Associate or any of its subcontractors while performing services pursuant to this BAA may cause irreparable harm to Covered Entity for which Covered Entity will be entitled, if it so elects to seek injunctive or other equitable relief.
6. Termination of Relationship.
7. Immediate Termination and Cure. Covered Entity may immediately terminate its relationship with Business Associate upon written notice to Business Associate without damages, liability or penalty to Business Associate if Covered Entity determines that Business Associate has violated a material requirement related to HIPAA. Covered Entity, at its option and within its sole discretion, has the right to take reasonable steps to cure the breach and/or may (a) allow Business Associate to take steps to cure the breach, and (b) in the event of such a cure, elect to keep the this BAA and relationship in full force and effect.
8. PHI Obligations upon Termination or Expiration. Unless Business Associate is required by law to maintain PHI, Business Associate shall return or destroy (and not retain any copies of) all PHI in its possession or under its control within thirty (30) days after the termination/expiration of this BAA. Business Associate shall seek and obtain written instructions from the Covered Entity regarding whether to return or destroy the PHI. If Business Associate is unable to return PHI and if requested to destroy the PHI and destruction is not feasible, then Business Associate shall notify Covered Entity of the reasons for being unable to return or destroy PHI in writing and must extend the protections of this BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. Business Associate shall not transfer possession, custody or control of Covered Entity’s PHI to any other person or entity without prior written approval of Covered Entity. If at any time Business Associate determines it is unable to protect the Covered Entity’s PHI in accordance with the terms of this BAA, Business Associate shall destroy all Covered Entity PHI and all copies thereof and promptly provide proof of such destruction to Covered Entity.
9. Covered Entity may terminate this BAA effective immediately, if (a) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy laws or (b) there is a finding or stipulation that Business Associate has violated any standard or requirement of HIPAA or other security or privacy laws in any administrative or civil proceeding in which Business Associate is involved.
10. Termination of Other Agreements.If this BAA is terminated for any reason, Covered Entity may terminate any or all other agreements between the parties which involve the use or disclosure of PHI. This provision shall supersede any termination provision to the contrary which may be set forth in any other agreement.
11. Offshore Disclosure and Written Authorization.  Prior express written authorization from Covered Entity, in addition to this BAA, is required for Business Associate to access, store, share, maintain, transmit or  use or disclose PHI in any form via any medium with any entity or person, including the Business Associate’s employees and subcontractors, beyond the boundaries and jurisdiction of the United States.

1. Information System Access. This paragraph only applies in cases where the Business Associates’ employees and/or its subcontractors’ employees will be provided within continuous log-on access to the Covered Entity’s Information System:
2. Policies and Procedures. Business Associate agrees to comply with all of the Covered Entity’s Information Systems (network, systems or applications) policies and procedures applicable to accessing, using or connecting to any Covered Entity Information System.

In cases where the Business Associate has log-on access to Covered Entity’s Information Systems, including Nexus, the policies and procedures are posted and available on the Trinity Health’s Nexus site. Otherwise, the Covered Entity will provide its Information System policies and procedures in advance to the Business Associate.

1. Security Codes and Passwords. Business Associate agrees that its employees will only use their access security codes or passwords to perform their duties under this BAA and that employees are strictly prohibited from disclosing their security codes or passwords to anyone, including family, friends, fellow workers (other than the system security administrator), supervisors, and subordinates for any reason. Business Associate agrees its employees will keep their security codes and passwords in confidence and not misuse or attempt to alter Covered Entity’s Information System in any way.
2. Use of Access. Business Associate agrees to use its access to Covered Entity’s Information Systems and Confidential Information only for treatment, payment and operations purposes permitted by HIPAA for Individuals covered under the Plan or to perform services for Covered Entity. Business Associate will access, use or disclose Individual or business information obtained using access to the Information Systems only for the legitimate health care purposes of the Business Associate or to perform services for Covered Entity, and will only use or disclose the minimum necessary amount of information needed for the purposes identified.
3. Training. Business Associate will provide training to its employees and subcontractors on their responsibilities for proper use of Covered Entity’s Confidential Information and Information Systems. Upon request, Covered Entity will make available to Business Associate its educational brochure, “Information Privacy and Security: Your Responsibilities”, in an effort to assist Business Associate in training its employees’ and its permitted subcontractors’ compliance with respect to its obligations under this BAA.
4. Confidentiality Agreement for Individuals. Business Associate will require each of Business Associate’s employees and subcontractors with continuous log-on access to Covered Entity’s Confidential Information and Information Systems to sign and return the Covered Entity’s “Confidentiality Agreement” prior to being given continuous log-on access to the Information Systems (e.g., login ID and password).
5. Annual Review, Suspension and Termination of Access.

a. Business Associate will cooperate with Covered Entity in the timely suspension or termination of access of any of its employees and/or subcontractors who no longer need access to Covered Entity’s Information System to carry out his/her job functions. Business Associate will complete an annual review of all employees and subcontractors of Business Associate in an effort to identify individuals who no longer need such access.

b. Business Associate will immediately suspend or terminate its employee’s and/or subcontractor’s access to Covered Entity’s Information Systems and/or connection to a Covered Entity Network in the event of a suspected or actual violation of this BAA, and will not reinstate access and/or connection privileges until Covered Entity has agreed in writing to the reinstatement of these privileges.

c. Business Associate acknowledges that Covered Entity has, at its sole discretion, the right to immediately terminate any of the Business Associate’s employees and/or subcontractors right to access to any aspect of Covered Entity’s Information Systems and/or Network connection in the event of Business Associate’s improper use of Covered Entity’s Information System and/or Network connection, Business Associate’s failure to maintain the confidentiality of Covered Entity business information or any PHI, failure to maintain Individual privacy or failure to safeguard and protect the security of the Information Systems and/or Network connection, or Covered Entity’s PHI or business information.

1. Additional Obligations for Entities Permitted to Have Administrative Authority (Gatekeeper). In instances where the Business Associate is permitted to have administrative authority by Covered Entity to approve or revoke access to Covered Entity’s Information Systems, the Business Associate agrees that it will only grant access to persons eligible under Covered Entity’s policies and will not approve and request access to Covered Entity’s Information Systems for individuals other than its own employees, temporary staff members, credentialed physicians and students without the prior written approval of Covered Entity. Access by all other subcontractors requires prior written approval of Covered Entity.
2. Network Connection. This paragraph only applies in cases where the Business Associate is permitted to access Covered Entity Confidential Information via a network connection (the “Covered Entity Network”), the following provisions apply:
3. Personal Benefit. Business Associate shall not at any time or in any manner, either directly or indirectly, use for the personal benefit of Business Associate, distribute, sell, market or commercialize Covered Entity Confidential Information, create derivative products or applications based on Covered Entity Confidential Information or otherwise use Covered Entity Confidential Information in any manner not expressly permitted by this BAA.
4. Permitted Purposes of Connection**.**  Business Associate will use or disclose PHI obtained from the Covered Entity Network only for the legitimate health care purposes of

a. Treatment, payment and healthcare operations of the Business Associate if it is a covered entity; and/or

b. To perform services for Covered Entity related to treatment, payment and operations, and/or

1. Survival. The respective rights and obligations of the parties under this BAA, including without limitation the obligations of the Business Associate under Section Termination of Relationship, shall survive termination of the BAA to the extent necessary to fulfill their purposes.
2. Prior Business Associate Agreements. This BAA shall supersede any prior business associate agreements between Business Associate and Covered Entity.
3. Interpretation. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA.
4. Notices. All notices pertaining to this BAA shall be sent by certified mail, delivered by courier, or transmitted by facsimile and confirmed in writing (sent by air courier or certified mail) to a party at such address as the parties may agree.
5. No Third Party Beneficiaries. This BAA shall not create any additional rights for any third party beneficiary who may be receiving benefits or services pursuant to the terms and conditions of Covered Entity.

**COVERED ENTITY (TRINITY HEALTH CORPORATION, as the sponsor of and on behalf of the [Trinity Health Corporation Welfare Benefit Plan] [Trinity Health Retiree Medical Plan (Grandfathered)]**

Signature:

Name:

Title:

Date:

**BUSINESS ASSOCIATE**

Signature:

Name:

Title:

Date:

**BUSINESS ASSOCIATE**

Type of Service Provided to Covered Entity:

Website URL

1st Contact Person 2nd Contact Person

Name: Name:

*Title: Title:*

Telephone #: Telephone #:

Street Address (Suite # if any) Street Address (Suite # if any)

City, State, Zip Code City, State, Zip Code

Email: Email:

Fax #: Fax #:

Please send a copy of the fully executed agreement to:

Trinity Health Corporation

Attn: Legal Department

20555 Victor Parkway

Livonia, MI 48152