******

**Human Resources Operating Procedure No. 135**

**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:

***Privacy Official***

***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 establish the position of the Privacy Official for the Plan and set forth the responsibilities pertaining to that position. If the regulations under HIPAA are changed by HHS the Plan will follow the revised regulations.

**PROCEDURES**

1. ***Privacy Official***

The Privacy Official is the individual with oversight responsibility for the development, implementation, and operation of the Plan’s privacy compliance program. The Vice President, Total Rewards Benefits & Well-Being, has been designated as the Privacy Official.

1. ***Responsibilities of the Privacy Official***

In general, the Privacy Official’s job responsibilities include general responsibility for developing and implementing the Plan’s HIPAA Privacy Procedures to limit the Use and Disclosure of PHI. These responsibilities include, but are not limited, to the following tasks:

a. Establish a HIPAA privacy team charged with the development and implementation of a privacy compliance program;

b. Coordinate and facilitate the HIPAA privacy team’s activities;

c. Collaborate with the HIPAA privacy team, management, legal counsel, security, regulatory affairs and appropriate staff to create, implement, and monitor the Plan’s HIPAA Privacy Procedures, including policies for minimum necessary Use and Disclosure of PHI; access, inspection, and copying of PHI; amendment of PHI; accounting for disclosures of PHI; record-keeping procedures; and other administrative procedures;

d. Establish an internal privacy audit program to track certain non-routine disclosures of PHI;

e. Collaborate with other departments, divisions, and committees of the Plan Sponsor (such as accounting, legal, information systems, regulatory affairs, security and compliance) to ensure compliance with specific privacy requirements;

f. Assist in the development, implementation, and monitoring of Business Associate Agreements to ensure that all privacy requirements are adequately addressed;

g. Educating Workforce Members on the Plan’s HIPAA Privacy Procedures;

h. Establish and monitor a system for receiving questions and complaints regarding the HIPAA privacy compliance program;

i. Work with legal counsel, security and regulatory affairs to develop methods of investigating allegations of noncompliance with the Plan’s HIPAA Privacy Procedures, and, in conjunction with regulatory affairs and legal counsel, develop appropriate sanctions for noncompliance by employees and Business Associates;

j. Maintain current knowledge of applicable standards and, in conjunction with legal counsel, revise the privacy compliance program as necessary to reflect changes in the law or Plan Sponsor policy;

k. In conjunction with legal counsel and regulatory affairs, serve as an internal resource for all privacy-related matters and cooperate with external parties in any compliance reviews or investigations;

l. Delegate his or her duties and responsibilities under the privacy compliance program as appropriate;

m. Making the Plan’s HIPAA Privacy Procedures readily available/accessible to Workforce Members;

n. Providing on-going communication to Workforce Members regarding the Plan’s HIPAA Privacy Procedures;

o. Investigating and documenting HIPAA privacy related complaints/incidents according to standards and expectations established by the Trinity Health System Office Integrity and Audit Services HIPAA department;

p. Implementing and maintaining adherence to HIPAA, including privacy and security safeguards;

q. Conducting on-going compliance monitoring activities related to HIPAA, including conducting periodic risk assessments;

r. Continually analyzing and monitoring overall privacy compliance effectiveness;

s. Working in close collaboration with the Plan Sponsor’s Integrity and Compliance Officer and Security Official;

t. Ensuring that the Plan’s HIPAA Privacy Procedures are consistent with Trinity Health’s Organizational Integrity Program (i.e., Standards of Conduct); and

u. Serving as a resource person for HIPAA compliance for Workforce Members

***3. Delegation***

The Plan’s Privacy Official may delegate one or more of the responsibilities set forth in Section 2 of this Procedure to another individual as appropriate and necessary, but the Privacy Official remains responsible for ensuring compliance.

# 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.

**Compliance Committee** – The committee provides over-arching guidance to the THWBP in

relation to the compliance and security of the health plan. The committee is made up of a

diverse group of experts who support the THWBP .

**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 Human Resources Operating Procedure No. 122 (Minimum Necessary Use or Disclosure of

Protected Health Information).

**RELATED PROCEDURES AND OTHER MATERIALS**

* Human Resources Operating Procedure No. 120 (Use or Disclosure of Protected Health Information)
* Human Resources Operating Procedure No. 121 (Notice of Privacy Practices Related to the Use or Disclosure of Protected Health Information)
* Human Resources Operating Procedure No. 122 (Minimum Necessary Use or Disclosure of Protected Health Information)
* Human Resources Operating Procedure No. 123 (Business Associate Agreements)
* Human Resources Operating Procedure No. 124 (Limited Data Sets and De-Identified Data)
* Human Resources Operating Procedure No. 125 (Restrictions on the Use or Disclosure of Protected Health Information for Marketing Activities)
* Human Resources Operating Procedure No. 126 (Prohibition on the Sale of Electronic Health Records or Protected Health Information)
* Human Resources Operating Procedure No. 127 (Verification of Individuals Requesting Access to or Disclosure of Protected Health Information)
* Human Resources Operating Procedure No. 128 (Personal Representatives)
* Human Resources Operating Procedure No. 129 (Individual Rights Regarding Restrictions and Confidential Communications With Respect to Protected Health Information)
* Human Resources Operating Procedure No. 130 (Individual Rights Regarding Access to Protected Health Information)
* Human Resources Operating Procedure No. 131 (Individual Rights Regarding Accounting of Disclosures of Protected Health Information)
* Human Resources Operating Procedure No. 132 (Individual Rights Regarding Requesting Amendments to Protected Health Information)
* Human Resources Operating Procedure No. 133 (Administrative, Technical and Physical Safeguards of Participant Information)
* Human Resources Operating Procedure No. 134 (Breach Notification and Response)
* Human Resources Operating Procedure No. 136 (Workforce Educational Awareness and Training Related to the Privacy and Security of Protected Health Information)
* Human Resources Operating Procedure No. 137 (Refraining from Retaliatory Acts or Intimidating Acts Against Individuals)
* Human Resources Operating Procedure No. 138 (Complaints for Violation of the Privacy Rule)
* Human Resources Operating Procedure No. 139 (Mitigation of Harmful Effects)
* Human Resources Operating Procedure No. 140 (Sanctions)
* Human Resources Operating Procedure No. 141 (State Law Preemption)
* Human Resources Operating Procedure No. 142 (Research Involving Protected Health Information)
* Human Resources Operating Procedure No. 143 (Updates and Record Retention)
* Enterprise Information Security Procedures

**APPROVALS**

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

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