******

**Human Resources Operating Procedure No. 133**

**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:

***Administrative, Technical and Physical***

***Safeguards of Participant Information***

***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 administrative, technical and physical safeguards with respect to PHI maintained by the Plan. If the regulations under HIPAA are changed by HHS the Plan will follow the revised regulations.

**PROCEDURES**

1. ***E-mail Policy***

The Plan has the right to monitor both internal and external e-mails*.* E-mail shall be used for appropriate business purposes*.* The Plan will limit all Disclosure of PHI to Business Associates via e-mail, and only send encrypted transmissions pursuant to Section 10. below.

1. ***Security Protocols***

The Plan will designate security protocols for electronic or paper documents (including reporting a breach of confidentiality and disciplinary procedures for employees that breach confidentiality policies).

1. ***Storage of Claims and Appeals Documentation***

Paper claims and all appeals documentation should be stored in a file cabinet that is secured when not in use*.* Access to such cabinets will be limited to Workforce Members who require access to perform their job duties.No files containing PHI shall be left out on a desk overnight unless in a locked office. Claims and Appeals documentation may also be stored on a server where only authorized individuals have access.

1. ***Disposal Policy***

Whenever appropriate, Workforce Members who Use PHI will discard such information after Use unless otherwise required to be maintained under law or as necessary to administer the Plan. Workforce Members must affirmatively determine the appropriateness of discarding PHI prior to any such disposal, in accordance with Human Resources Operating Procedure No. 143 (Updates and Record Retention). If there is any doubt about the discarding of PHI, Workforce Members shall consult with the Privacy Official or his or her delegate. Workforce Members who discard PHI shall ensure that paper copies of such information are shredded prior to discarding.

1. ***Computer Access***

A password shall be required to log onto a computer and access electronic PHI and screens should be automatically turned off if activity does not occur for 15 minutes. Passwords must be at least eight characters long, a combination of numbers and letters, and must be changed every 120 days. Accounts will be locked out after five invalid attempts to log in. Workforce Members must not share their password information with anyone. Access shall be limited to Workforce Members who require access to perform their job duties.

1. ***Fax***

Any fax machine that will receive or transmit PHI must be in a secure location and be monitored regularly (e.g., every 30 minutes) for incoming documents. This separate fax will be located in a secured area. To transmit, print or download a fax that contains PHI, a Workforce Member must input his or her identification code into the fax machine. All outgoing faxes must include a confidentiality notice designating the document as potentially containing PHI.

1. ***Discussion Areas***

Access to physical areas where covered Individuals discuss benefit issues with Workforce Members should be limited. Conversations about individual benefit issues by individuals who are not involved in Payment or Healthcare Operations functions regarding that Individual are prohibited. Care should be taken to avoid conversations in public areas.

1. ***Computer Network***

Access controls (user-based, role-based or context-based) should be implemented and included in the administrative operations and system network controls. The Plan Sponsor will install a firewall to protect confidential information from Internet exposure. The Plan Sponsor will create a separate secure file on the server to house PHI that is either imaged or created by the Plan. Additionally, modifications should be made to limit access to the Plan eligibility component of the benefits administration system to Workforce Members only. Employees of the Plan Sponsor are prohibited from loading unauthorized software on to the Plan Sponsor’s computers.

1. ***Employment Terminations***

Upon final separation from employment of any employee of the Plan Sponsor within Human Resources, or the Plan, who has access to PHI, a Plan representative with access to PHI will collect all Plan Sponsor property and notify the Plan Sponsor’s IT Department to disable all accounts (e.g., passwords) of such employee. Upon final separation from employment of any employee of the Plan Sponsor who is not within Human Resources, or the Plan, who has access to PHI, the employee’s manager will collect all Plan Sponsor property and notify the Plan Sponsor’s IT Department to disable all accounts (e.g., passwords) of such employee.

1. ***Electronic Transmission***

Any and all electronic transmissions of data will be encrypted using a HIPAA-appropriate encryption protection system.

1. ***Disaster Recovery Program***

The Plan Sponsor will create a disaster recovery program for loss of data due to fire, vandalism, natural disaster or other system failure. This includes the frequent creation of a backup tape, and its offsite storage, to the extent appropriate.

1. ***Shredding***

After appropriate Use is complete, documents containing PHI will be shredded before disposal, subject to the time frames specified in Human Resources Operating Procedure No. 143 (Updates and Record Retention).

1. ***Hardware Disposal***

Prior to disposal, hard drives of all computers shall be erased so that no Plan data remains and none can be recovered by any known recovery method.

1. ***Audit Trails***

The Plan Sponsor will monitor access to information stored on its system through the use of audit trails.

1. ***Subcontractor Policy***

When the Plan subcontracts for services and the Plan Sponsor subcontractors have access to PHI, the Plan Sponsor will seek to verify that each subcontractor has procedures in place to reasonably safeguard PHI.

# 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.

**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.

**Healthcare Operations means** any of the following activities of the Covered Entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR § 3.20), population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities;

3. Except as prohibited under 45 CFR §164.502(a)(5)(i) (prohibited use of genetic information for underwriting), underwriting, enrollment, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);

4. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

6. Business management and general administrative activities of the entity, including, but not limited to:

a. Management activities relating to implementation of and compliance with the requirements of HIPAA;

b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;

c. Resolution of internal grievances;

d. The sale, transfer, merger or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that, following such activity, will become a Covered Entity, and due diligence related to such activity; and

e. Consistent with the applicable requirements of HIPAA, creating de-identified health information or a limited data set, and fund raising for the benefit of the Covered Entity.

**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.

**Payment** **means**:

1. The activities undertaken by:

a. Except as prohibited under 45 CFR §164.502(a)(5)(i) (prohibited use of genetic information for underwriting), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

b. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

2. The activities in paragraph 1. of this definition relate to the Individual to whom health care is provided and include, but are not limited to:

a. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication or subrogation of health benefit claims;

b. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance) and related healthcare data processing;

d. Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care or justification of charges;

e. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

f. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:

i. Name and address;

ii. Date of birth;

iii. Social security number;

iv. Payment history;

v. Account number; and

vi. Name and address of the healthcare provider and/or health plan.

**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.

**Treatment means** the provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

**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. 122 (Minimum Necessary Use or Disclosure of Protected Health Information)
* Human Resources Operating Procedure No. 123 (Business Associate Agreements)
* 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**