******

**Human Resources Operating Procedure No. 122**

**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:

***Minimum Necessary Use or Disclosure of***

***Protected Health 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**

To support the Plan’s commitment to covered Individual confidentiality, the Plan will ensure that the appropriate steps are taken to Use, Disclose, or request only the minimum amount of PHI necessary to accomplish the intended purpose of the Use, Disclosure, or request, as required under 45 CFR §§ 164.502(b) and 164.514(d), and other applicable federal, state, and/or local laws and regulations. If the regulations under HIPAA are changed by HHS the Plan will follow the revised regulations.

**PROCEDURES**

***1. Minimum Necessary – In General***

a. The Plan will make “reasonable efforts” to limit the use, disclosure, access to or requests for PHI to the Minimum Necessary.

b. The Plan’s Business Associates must comply with this Procedure.

c. This Procedure does not apply to:

i. Disclosure to or requests by a health care provider for Treatment;

ii. Uses or Disclosure made to the Individual who is the subject of the information;

iii. Uses or Disclosure pursuant to an Authorization by the Individual who is the subject of the information;

iv. Disclosure made to HHS;

v. Uses or Disclosures required by law; and

vi. Uses or Disclosure required for compliance with applicable requirements of HIPAA.

d. If practicable and required under the HITECH Act and its implementing regulations, the Plan will limit the Use, Disclosure, or request of PHI to that of a Limited Data Set (as defined in 45 CFR § 164.514(e)(2)) to meet the Minimum Necessary standard.

***2. Internal Use by the Plan***

a. The Plan has identified the following persons or classes of persons who need access to PHI to carry out their duties with respect to the Plan:

i. The following employees or classes of employees under the control of the Plan Sponsor who are responsible for Plan administrative functions, to the extent needed to perform the essential functions of their jobs:

a. Employees who work in Total Rewards Benefits with specific accountability for the Plan; and

b. Employees performing care management activities for the Plan; and

c. Clinical Consultants to the Plan.

The employees and classes of employees listed above are the Plan’s “Workforce Members.”

ii. The Administrator of the Plan and members of the Trinity Health Benefits Committee require access to PHI to perform certain functions with respect to the Plan, including claims, appeals and complying with its reporting and disclosure obligations..

iii. Employees in the Plan Sponsor’s legal, finance, accounting, IT and certain other departments require access to PHI to perform functions of their jobs.

b. The Plan has identified the categories or types of PHI needed:

i. Plan Sponsor employees identified in Section 4.a. above (“Plan Sponsor Employees”) will be trained in their particular department to recognize information that is necessary to perform the job and to avoid access to information that is not necessary.

ii. For example, when processing eligibility, a Plan Sponsor Employee may have access to all information necessary to make a determination as to whether the Individual is eligible to participate in the Plan and the effective date of his or her coverage.

iii. For example, when processing a claim for benefits under the Trinity Health Corporation 403(b) or 401(k) Retirement Savings Plan, including a claim for disability benefits, a Plan Sponsor Employee may not access PHI maintained by the Plan (or one of its Business Associates) without a written Authorization from the Individual.

c. The Plan has identified the conditions appropriate to access PHI.

i. The Plan Sponsor Employees must be trained on the Plan’s HIPAA Privacy Procedures before they may access PHI.

ii. Plan Sponsor Employees providing Plan administrative services may only access an Individual’s PHI when they are working on a Payment or Healthcare Operation issue involving the Individual. For example, Plan Sponsor Employees cannot view a file on which they are not working, unless access is necessary for purposes of assuring consistent and accurate claims administration.

iii. Plan Sponsor Employees may not discuss an Individual’s PHI unless it is necessary to perform a Payment or Healthcare Operation function. For example, Plan Sponsor Employees should not discuss interesting claims with employees who do not have a need to know the information.

***3. Routine Disclosures***

a. For Disclosures that the Plan makes on a routine basis, the Plan and the Plan Sponsor Employees will make reasonable efforts to limit the PHI Disclosed to the Minimum Necessary to accomplish the intended purpose(s) of the Disclosure.

b. The Privacy Official or his or her delegate will identify Disclosures of PHI that the Plan and the Workforce Members make on a routine, recurring basis.

c. The Plan is responsible for creating standards to reasonably ensure that routine Disclosures only include the Minimum Necessary PHI.

i. Each standard developed under this Section will address the following:

a. The standard will set forth the type of PHI that can be Disclosed;

b. The standard will identify the types or categories of persons to whom the PHI identified in the standard can be Disclosed; and

c. The standard will identify any applicable conditions to providing the Disclosure.

ii. The Privacy Official is responsible for making the final determination as to whether a Disclosure can be categorized as “routine and recurring.”

***4. Non-Routine Disclosures***

a. The Privacy Official or his or her delegate must approve any non-routine Disclosures. Each non-routine Disclosure must be reviewed on an individual basis. The criteria for reviewing a non-routine Disclosure are as follows:

i. The non-routine Disclosure must be necessary to allow the Plan to carry out its obligations under ERISA and the governing Plan documents;

ii. The non-routine Disclosure must be limited to the information reasonably necessary to accomplish the purpose of the Disclosure;

iii. The non-routine Disclosure must be otherwise consistent with the Plan’s HIPAA Privacy Policies and Procedures;

iv. The non-routine Disclosure must not be prohibited by HIPAA; and

v. A request for a non-routine Disclosure that is accompanied by an Individual’s written Authorization that is compliant with HIPAA will be honored in a manner consistent with the Plan’s HIPAA Privacy Policies and Procedures.

b. When receiving a request for PHI from one of the following categories of persons, the Plan and the Workforce Members may rely on the judgment of the requestor as to the minimum amount of information that is necessary for the stated purpose(s), if such reliance is reasonable:

i. Public official or agency for a Disclosure that is permitted under HIPAA if the public official represents that the information requested is the Minimum Necessary for the stated purpose(s);

ii. Health plan, healthcare clearinghouse, or healthcare provider that is covered by HIPAA;

iii. The information is requested by a professional who is a Workforce Member or is a Business Associate of the Plan for purposes of providing professional services to the Plan, if the professional represents that the information requested is the Minimum Necessary for the stated purpose(s); or

iv. The Individual.

Requests for Disclosures by one of the persons listed above does not require individual review by the Privacy Official or his or her delegate. However, in the event a Plan Sponsor Employee believes that a request for a Disclosure involving PHI from a person listed above is not the Minimum Necessary, such Plan Sponsor Employee will raise his or her concerns with the Privacy Official or his or her delegate. The Privacy Official or his or her delegate is responsible for evaluating such requests for Disclosure and determining whether it is reasonable for the Plan to rely on such request. The Privacy Official may contact the person making the Disclosure request to discuss the concerns raised by the request.

***5. Requests***

###### a. When requesting PHI from another Covered Entity, the Plan and the Workforce Members will make reasonable efforts to limit the request to the minimum amount of PHI which is reasonably necessary to accomplish the intended purpose(s).

###### b. For requests that are made on a recurring and routine basis, the Plan and the Workforce Members must limit the PHI requested to the amount reasonably necessary to accomplish the purpose(s) for which the request is made.

###### i. The Privacy Official is responsible for identifying requests for PHI that are made on a routine, recurring basis. The Privacy Official is responsible for creating standards to be applied to reasonably ensure that routine requests for Disclosures of PHI are limited to the Minimum Necessary.

###### ii. Each standard developed under this Section will address the following:

###### I. The standard will set forth the type of PHI that can be requested;

###### II. The standard will identify the types or categories of persons from whom the PHI identified in the standard can be requested; and

###### III. The standard will identify any applicable conditions to making the request.

###### iii. The Privacy Official is responsible for ensuring that the standards for routine requests for PHI are created and implemented as required under this Section and for making the final determination as to whether a request for PHI can be categorized as “routine and recurring.”

###### c. If a request for PHI cannot be categorized as “routine and recurring,” then the following requirements apply:

###### i. All requests for PHI that do not qualify as “routine and recurring,” must be reviewed on an individual basis to determine that the PHI sought is limited to the Minimum Necessary to accomplish the purpose(s) for which the request is made. The Privacy Official will be responsible for reviewing such non-routine requests for PHI.

###### ii. The Privacy Official is responsible for developing criteria to be applied to analyze non-routine requests for PHI to determine that only the Minimum Necessary PHI is requested.

###### iii. All non-routine requests for PHI will be forwarded to the Privacy Official for review and approval prior to making the request.

***6. Rules for Entire Medical Record***

The Plan may not Use, Disclose, or request an entire medical record, except when the Plan, in consultation with a health care professional in the exercise of his or her professional judgment, determines that the entire medical record is specifically justified as the Minimum Necessary to accomplish the purpose(s) of the Use, Disclosure, or request.

# 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.

**Authorization means** the written permission from an Individual that permits the Plan to Use or Disclose PHI for purposes beyond the scope of Treatment, Payment or Healthcare Operations.

**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.

**Minimum Necessary means** a limited data set or alternatively, if the limited data set is not sufficient, then the least amount of PHI necessary to accomplish the intended purpose of the Use, Disclosure or request.

**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

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 this Procedure.

**RELATED PROCEDURES AND OTHER MATERIALS**

* Human Resources Operating Procedure No. 120 (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)
* Enterprise Information Security Procedures
* Authorization for Use and Disclosure of Protected Health Information

**APPROVALS**

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

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