******

**Human Resources Operating Procedure No. 134**

**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:

***Breach Notification and Response***

***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 outline a systematic process designed to notify affected Individuals of any breach of privacy or security with respect to any unsecured PHI that is received, created, retained, Used or Disclosed by the Plan. If the regulations under HIPAA are changed by HHS the Plan will follow the revised regulations.

* + - 1. ***General – Identification and Notification of a Breach***

1. Except for the instances explicitly excluded from the definition of Breach, an acquisition, access, Use, or Disclosure of PHI in a manner not permitted under HIPAA is presumed to be a Breach unless the Plan or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who Used the PHI or to whom the Disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

1. Upon discovering a potential Breach, in order to determine if the presumption of the Breach should be confirmed, the Plan shall conduct an analysis that includes the above factors. The analysis should be fact specific.
2. The Plan must document its Breach analysis and maintain such documentation for a minimum of six (6) years.
3. In the case of a Breach of unsecured PHI for which the Plan is responsible as a Covered Entity, the Plan shall notify the affected Individuals, without unreasonable delay and in no case later than 60 calendar days following the discovery of the Breach.

i. A Breach is considered discovered as of the first day on which the Breach is known to the Plan (including any person, other than the individual committing the Breach, who is an employee, officer, or other agent of the Plan Sponsor, another entity that is a participating employer in the Plan or the Plan), or should have been known to the Plan through the exercise of reasonable diligence. If a Business Associate of the Plan is acting as an agent of the Plan and discovers a Breach, the Business Associate’s discovery of the Breach will be imputed to the Plan. In that case, the Plan’s discovery of the Breach will be the first day on which the Breach was known to the Business Associate, not the date when the Business Associate notified the Plan of the Breach. If a Business Associate is acting as an independent contractor to the Plan and discovers the Breach, the Plan’s discovery of the Breach will be the first day on which the Business Associate notified the Plan of the Breach. The Plan shall ensure that all employees and agents are adequately trained to discover and report potential Breaches.

1. All Plan Sponsor and Plan employees and agents are expected to work collaboratively to timely and accurately report any Breach of Unsecured PHI to the Privacy Official and according to this Procedure, HIPAA, HITECH, and any and all other applicable federal and state laws and regulations (to the extent such state laws and regulations are not preempted by federal law, including ERISA). The Privacy Official shall maintain all documentation related to any Breach of Unsecured PHI for a minimum of six (6) years from the date of notification provided hereunder.
2. ***Notification to Affected Individuals***

a. After a prompt internal investigation and Breach analysis, without unreasonable delay and in no case later than 60 calendar days of the Plan discovering a Breach, the Plan Sponsor or its authorized delegate shall provide written Breach notification to each Individual whose Unsecured PHI has been, or is reasonably believed by the Plan to have been accessed, acquired, Used, or Disclosed as a result of such Breach. In the event a Breach is caused by a Business Associate of the Plan, and upon mutual agreement of the Plan and the Business Associate, the Plan may delegate the provision of the written Breach notification to affected Individuals to the Business Associate that suffered or is responsible for the Breach or to another Business Associate of the Plan.

b. Written notification should be sent by first-class mail to the last known address of the affected Individual or by electronic mail provided the affected Individual has agreed to receive electronic notice and such agreement has not been withdrawn. The notification may be provided in one or more mailings as information becomes available. If the Plan knows the affected Individual is deceased, notice must be sent to the last known address of the affected Individual’s next of kin or personal representative unless the Plan does not have the address for the next of kin or personal representative.

c. If the Plan does not have sufficient contact information for some or all of the affected Individuals, the Plan must provide substitute notice for the unreachable Individuals in accordance with HIPAA regulations, 45 CFR §164.404(d)(2).

d. If the Plan determines that the affected Individual and/or law enforcement should be notified urgently of a Breach because of possible imminent misuse of Unsecured PHI, the Plan may, in addition to providing notice as outlined in Section 2.a. and b., above, notify the affected Individual and/or law enforcement by telephone or other appropriate means.

e. If a law enforcement official states that a notification would impede a criminal investigation or cause damage to national security, the Plan or its Business Associate shall:

i. If the statement is in writing and specifies the time for which a delay is required, delay such notification for the time period specified by the official; or

ii. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification temporarily but no longer than 30 days from the date of the oral statement, unless a written statement as described in i., above, is submitted during that time.

f. Notice of the Breach must include:

i. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

ii. A description of the types of Unsecured PHI that were involved in the Breach, such as full name, social security number, date of birth, home address, account number, health plan or insurance information, and medical information such as diagnosis or disability codes. Only the generic type of PHI should be listed in the notice (i.e., date of birth rather than the Individual’s actual birth date).

iii. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach.

iv. A brief description of what the Plan is doing to investigate the Breach, mitigate the harmful effects of the Breach, if possible, and to protect against any further Breaches.

v. Contact procedures for Individuals to ask questions or learn additional information, including a toll-free telephone number, an e-mail address, web site, or postal address.

vi. Any other information required by the HIPAA regulations.

g. The Plan must maintain documentation that all required notifications were made for a minimum of six (6) years.

***3. Reporting to Media***

In the case where a single Breach event affects more than 500 residents of the same state or jurisdiction, the Privacy Official, in consultation with the Plan Sponsor’s media services department or similar individual, such as a public information officer, will provide notice to prominent media outlets in that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days of the Plan discovering the Breach. Such media notification must include the information required in the notification to affected Individuals and should be made in addition to sending an individual notice to affected Individuals.

***4.*** ***Mandatory Notification to HHS***

a. If a single Breach event affects 500 or more Individuals regardless of the state or jurisdiction, the Plan must, contemporaneously with the notice provided to affected Individuals, notify the Secretary of HHS. This notice must be submitted electronically by using the Breach Notification Form located at this website address: <http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html> (or at any address located in subsequent guidance). The Plan must complete all information required on the Breach Notification Form. If the Plan has submitted a Breach Notification Form to the Secretary of HHS and later discovers additional information to report, the Plan may submit an additional form, checking the appropriate box to signal that it is an updated submission. Notice to the Secretary of HHS should be made in addition to sending an individual notice to affected Individuals. Any notification to the Secretary of HHS must be approved by the Plan Sponsor’s legal and media services departments prior to providing the notification; provided, however, that any required notification will be provided in the time and manner required by applicable law.

b. If a Breach is with respect to less than 500 Individuals, the Plan will document the Breach in the Plan Sponsor’s incident documentation system (Compliance 360). The Plan will notify/report the Breaches to HHS no later than sixty (60) days after the end of each calendar year. Notice of Breaches affecting less than 500 Individuals must be submitted electronically by using the Breach Notification Form located at this website address: <http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html> (or at any address located in subsequent guidance). A separate form must be completed for every Breach that has been discovered and the Plan has logged during the calendar year. The Plan must complete all information required on the Breach Notification Form. If the Plan has submitted a Breach Notification Form to the Secretary of HHS and later discovers additional information to report, the Plan may submit an additional form, checking the appropriate box to signal that it is an updated submission. Any notification to the Secretary of HHS must be approved by the Plan Sponsor’s legal and media services departments prior to providing the notification; provided, however, that any required notification will be provided in the time and manner required by applicable law.

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.

**Breach means** the acquisition, access, use, or disclosure of PHI received, created, retained, Used or Disclosed by the Plan as a Covered Entity, in a manner not permitted under HIPAA, which compromises the security or privacy of the PHI. The determination of whether any Breach or potential Breach compromises the security or privacy of the PHI shall be made in good faith by the Plan. The term “Breach” does not include:

1. Any unintentional acquisition, access, or Use of PHI by a Workforce Member or person acting under the authority of the Plan or Business Associate of the Plan, if such acquisition, access, or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under HIPAA;

2. Any inadvertent Disclosure by a person who is authorized to access PHI at the Plan Sponsor under the Plan or a Business Associate of the Plan, to another person authorized to access PHI at the Plan Sponsor under the Plan or the same Business Associate of the Plan, or an organized health care arrangement in which the Plan participates, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under HIPAA; or

3. A Disclosure of PHI where the Plan or Business Associate of the Plan has determined or has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

**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.

**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.

**Unsecured PH**I **means** PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in guidance published by the Secretary of HHS.

**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
* Sample Breach Notification Letter to Affected Individuals
* Breach Notification Form (located at <http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>)

**APPROVALS**

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

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

**08/12/2015**

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

SAMPLE BREACH NOTIFICATION LETTER TO AFFECTED INDIVIDUALS

\*\*\*Letter Date\*\*\*

\*\*\*IF Breach Notification Distribution Method = “First-Class U.S. Mail”\*\*\*

\*\*\*Individual’s First Name\*\*\* \*\*\*Individual’s Last Name\*\*\*

\*\*\*Individual’s Mailing Address\*\*\*

\*\*\*City\*\*\*, \*\*\*State\*\*\* \*\*\*Zip Code\*\*\*

\*\*\*Individual’s Email Address\*\*\*

\*\*\*Individual’s Phone Number\*\*\*

Re: Breach of Protected Health Information

Dear \*\*\*Individual’s Courtesy Title\*\*\* \*\*\*Individual’s Last Name\*\*\*:

We are writing to you because of a recent incident at involving the [potential] unauthorized access, use or disclosure of certain protected health information (“PHI”) maintained as part of the records of the [Trinity Health Corporation Welfare Benefit Plan] [Trinity Health Corporation Retiree Benefit Plan (Grandfathered)] (the “Plan”).

[Describe what happened, including:

* the date of the Breach and the date of the discovery of the Breach, if known;
* a description of the types of Unsecured PHI that were involved in the Breach, such as full name, social security number, date of birth, home address, account number, health plan or insurance information, and medical information such as diagnosis or disability codes. Only the generic type of PHI should be listed in the notice (*i.e.*, date of birth rather than the patient’s actual birth date);
* any steps the individual should take to protect him/herself from potential harm resulting from the Breach;
* a brief description of what the Plan is doing to investigate the Breach, mitigate the harmful effects of the Breach, if possible, and to protect against any further Breaches; and
* contact procedures for the individual to ask questions or learn additional information, including a toll-free telephone number, an e-mail address, web site, or postal address.]

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact the Privacy Official that the Plan has designated and appointed to ensure that Plan-related PHI is appropriately protected at:

Trinity Health Corporation Welfare Benefit Plan

Trinity Health Corporation Retiree Benefit Plan (Grandfathered)

Attn: Privacy Official

20555 Victor Parkway

Livonia, MI 48152

Phone Number: 734-343-1000

Sincerely,