HIPAA-05: Breach Notification Policy

Effective Date:	12-01-2015	Last Revised:	7-17-2017

Scope of Policy

This policy governs Breach Notification for **TCS**. All personnel of **TCS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Assumptions

- ❑ **TCS** must comply with HIPAA and the HIPAA implementing regulations concerned with notifications to patients and consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.
- ❑ Compliance with HIPAA's breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.
- ❑ Timely notifications to consumers about breaches of individually identifiable health information can help reduce or prevent identity theft and fraud.
- ❑ Timely notifications to consumers about breaches of individually identifiable health information can help protect our business and reputation.
- ❑ Only breaches of "unsecured" (unencrypted or not destroyed) protected health information trigger HIPAA's breach notification requirements.

Definitions

As used within the HIPAA Final ("Omnibus") Rule, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted **under subpart E of this part which compromises the security or privacy of the protected health information**.

- ❑ Breach excludes:

  a) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, 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 subpart E of this part.

  b) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

  c) A disclosure of protected health information where a covered entity or business associate 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.

- ❑ Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a

low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

a) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
b) The unauthorized person who used the protected health information or to whom the disclosure was made;
c) Whether the protected health information was actually acquired or viewed; and
d) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

Policy Statement

- ❑ It is the Policy of **TCS** to provide timely notifications to affected (patients and/or) consumers about breaches of individually identifiable health information.
- ❑ **TCS** shall notify individuals when a reportable breach is discovered. A breach is treated as "discovered" by the **TCS** the first day on which such breach is known or should reasonably have been known to any employee or agent of **TCS**, other than the person who committed the breach.
- ❑ Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the breach, unless law enforcement requests a delay.

Procedures

- ❑ Breach Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
- ❑ First class mail shall be the default method of notification. **TCS** may use e-mail if requested by the individual, or substitute notice via our website or local print or broadcast media if we do not have current contact information.
- ❑ **TCS** must notify major local media outlets of a breach affecting more than 500 individuals.
- ❑ Business Associates of **TCS** are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to **TCS**'s designated Privacy Officer.
- ❑ Business Associate contracts, whether existing or new, shall have corresponding breach notification requirements included in them.
- ❑ Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to **TCS**'s Sanction Policy.
- ❑ All breach-related activities and investigations shall be thoroughly and timely documented in accordance with **TCS**'s Documentation Policy.