HIPAA-45 Change Control Policy, Procedure and Form

Effective Date:	7-17-2017	Last Revised:	7-17-2017

Scope of Policy

This policy governs the management of changes to the information technology infrastructure by any member of the **TCS**. All personnel of **TCS** and IT vendors 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.

The purpose of the policy is to develop the appropriate safeguards to protect ePHI and other sensitive data during the change management process.

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements to safeguard ePHI and provide access to patient
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- The risk of introducing significant changes to the production environment must be managed through an appropriate level of documentation, authorization, planning, and testing. These changes could potentially impact the stability or performance of the company's IT production environment. By using a series of standardized and repeatable procedures and actions, the Company will be able to better manage any changes to the IT infrastructure in such a way that any negative impact is minimized.
- Full compliance with HIPAA reduces the overall risk to Protected Health Information (PHI), and reduces the risk to confidential health data.

Policy Statement

- Any new information system upgrade or product installation has the potential to introduce risk factors for **TCS** (e.g., system downtime, data loss and impact on patient services). This Change Control Policy requires that an orderly procedure be established for managing the risks associated with making changes to the network computing environment (i.e., Active Directory, Exchange, OS Patches, etc.), Key applications systems, and network infrastructure.
- This will be accomplished by requiring any change to be carefully assessed for potential risks and developing an appropriate contingency plan (e.g., rollback procedures) in the event something goes wrong.

Change Management Process

The process that is to be used for requesting and managing these changes is described as follows and involves defined roles:

- Roles - The following are the key roles involved in the Change Control process. One individual may be responsible for several roles as well as several individuals may be fulfilling a single role. The Executive Director is responsible for managing the execution of the Change Control process with the assistance of the HIPAA Compliance Committee.

    1. *Change Requestor* - The Change Requestor originates the request by submitting a Request For Change (RFC) to the Change Control Manager. This functional role may be filled by the manager authorizing the project and/or the IT staff person who has recommended.

2. *Change Control Manager* - The Change Control Manager (Executive Director or designee) manages the process for all requests and reviews each request for completeness. The Change Control Manager verifies that: a) the stated objectives of the request are valid; b) an acceptable risk management plan has been developed,; c) and must approve any RFC. The Change Control Manager has the discretion to deny requests that are not consistent with TCS policy or best practices.

3. *Change Implementer* - The Change Implementer (e.g., NetGain SE) makes the necessary changes as requested in the RFC and notifies any other affected parties if corresponding changes need to be made. Changes are implemented into production by the Change Implementer.

4. *Change Control Team* – In some instances, the Change Control Manager may elect to establish a Change Control Team to manage the objectives of the specific request. The team could be comprised of members representing the technical, operational and management areas. This team would meet as needed to review, approve/reject all proposed changes, and schedule change actions.

RFC Procedures: (please review and personalize as you feel appropriate for TCS)

1. A Request For Change Form (RFC) must be submitted to the Change Control Manager.
2. If the RFC is an emergency that has minimal risk impact and minimal cost, the Change Control Manager and IT staff can authorize based on a review of the RFC form; (see item 7 below). If the RFC is not an Emergency Change, an appropriate Change Control Team may be formed to review the scope and impact of the requested change.
3. An impact analysis is performed (by the Change Control Manager or a member of the Change Control Team) to determine what applications are affected by the change, if an outage is required and to determine the approximate costs and risks associated with the request. A back-out plan should also be developed and included in the impact analysis to ensure that unsuccessful changes or undesirable results do not adversely impact business processes.
4. The Change Control Team will meet as needed to review proposed changes. The Change Control Manager is the coordinator of the Change Control Team.
5. If a request is denied, the requestor is notified in writing.
6. Requests that are approved are categorized by priority (critical or normal), a Change Implementer is assigned, an implementation date is determined, and responsibility for end user communications is assigned.
7. Emergency changes and IT changes: In the event of an emergency requirement for a change, the Change Control Manager must approve a change prior to implementation and document reason for change, implementation notes and appropriate testing. The Change Control Manager will review all approved emergency changes and IT changes periodically with the IT Manager.
8. Once completed and tested, the documentation of the project and change control process shall be retained in the TCS HIPAA Documentation files.