Policy Title: HIPAA Data Backup and Contingency Planning

Number: TD-QMP-7008

Subject: Creating secondary storage and contingency planning for the protection of electronic HIPAA information

Primary Department: TennDent/Quality Monitoring/Improvement
Secondary Department: TennDent/IT

Effective Date of Policy: 9/23/2011
Prior Policy or Cross Reference(s): 10/1/2010

Last Reviewed by TennDent Quality Monitoring/Improvement Committee: 9/23/2011
Date Policy Last Revised: 9/23/2011

Review Frequency: Annually
Next Scheduled Review: 7/1/2012

TennDent Quality Monitoring/Improvement Committee Approval: On File
Approval Date: 9/23/2011

Scope:

TennDent has adopted this policy to ensure that its response to an emergency or other occurrence that damages systems that contain EPHI complies with the Security Regulations.

Purpose:

TennDent is committed to conducting business in compliance with all applicable laws, regulations and TennDent policies. This Policy covers the procedures that TennDent will develop for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains Electronic Personal Health Information (EPHI) is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster Recovery Planning
- Emergency mode operation plan

Authoritative Reference:

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) HIPAA Security Rule [HIPAA Administrative Safeguards] (see § §164.308(a)(7)]
Policy:

1. Applications and Data Criticality Analysis
   a. TennDent will assess the relative criticality of specific applications and data within TennDent for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.
   b. The assessment of data and application criticality will be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

2. Data Backup Plan
   a. TennDent will establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all EPHI determined to be medium and high risk.
   b. The Data Backup Plan must apply to all medium and high-risk files, records, images, voice or video files that may contain EPHI.
   c. The Data Backup Plan must require that all media used for backing up EPHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
   d. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard the EPHI in an appropriate manner.
   e. Data backup procedures outlined in the Data Backup Plan must be tested on a periodic basis to ensure that exact copies of EPHI can be retrieved and made available.
   f. With medium and high risk EPHI TennDent must submit its Data Backup Plan to the Information Security Officer for approval.

3. Disaster Recovery Plan
   a. To ensure that TennDent can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing EPHI, TennDent will establish and implement a Disaster Recovery Plan pursuant to which it can restore or recover any loss of EPHI and the systems needed to make that EPHI available in a timely manner.
   b. The Disaster Recovery Plan should include procedures to restore EPHI from data backups in the case of a disaster causing data loss.
   c. The Disaster Recovery Plan should include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.
   d. The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.
   e. The disaster recovery procedures outlined in the Disaster Recovery Plan must be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.
   f. TennDent with medium and high risk EPHI must submit its Disaster Recovery Plan to the Information Security Officer for approval.

4. Emergency Mode Operation Plan
a. TennDent will establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.
b. Emergency mode operation procedures outlined in the Emergency Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
c. With medium and high risk EPHI TennDent must submit its Emergency Operation Plan to the Information Security Officer for approval.

Violations
Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Related Policies and Procedures:

Document and Records Management Policy
Document and Records Management Procedure
HIPAA Data Backup and contingency Planning Policy
HIPAA Data Backup Procedures

Related Documents:

Data Backup Plan
Disaster Recovery Plan
Emergency Operation Plan
Business Associate Agreement