

| | |
|---|---|
| Policy Title: HIPAA Facility Access Controls Number: TD-QMP-7014 | |
| Subject: Ensuring that physical access to Electronic Protected Health Information (EPHI) is appropriately limited. | |
| Primary Department: TennDent/Quality Monitoring/Improvement | Secondary Department: TennDent/Administration |
| 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 staff, employees of Delta Dental of Tennessee (DDTN)

Purpose:

TennDent is committed to conducting business in compliance with all applicable laws, regulations and TennDent policies. This Policy covers the procedures that will limit physical access to electronic information systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

Authoritative Reference:

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) HIPAA Security Rule [HIPAA Physical Safeguards] [see §164.310(a)(1) & (2)]

Policy:

1) Facility Security Plan

TennDent will create and maintain a Facility Security Plan that outlines and documents its procedures to safeguard all facilities, systems, and equipment used to store EPHI against

unauthorized physical access, tampering, or theft. The Facility Security Plan must include the following components:

- (1) Contingency Operations – procedures that allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan. (See HIPAA Security Policy – Data Backups and Contingency Planning Policy)
- (2) Access Control and Validation – procedures to control and validate Workforce member's access to facilities based on their role or function.
- (3) Physical Access Records – procedures to log physical access to any facility containing medium and high risk EPHI-based systems. Examples of facilities requiring physical access records are computer, telephone and system rooms.
- (4) Maintenance Records – procedures to document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.

2) Workforce Access Controls

- a) TennDent will establish and implement appropriate procedures to control and validate TennDent employee access to all facilities used to house EPHI based systems.
- b) TennDent will adopt appropriate access control mechanisms to control physical access to all facilities containing EPHI-based systems. Code locks, badge readers, and key locks are examples of physical access control mechanisms.

3) Visitor Access Controls

- a) TennDent will establish and implement procedures to control, validate, and document visitor access to any facility used to house EPHI based systems. Visitors include vendors, repair personnel, and other non-Workforce members.
- b) All visitors who require access to facilities containing EPHI-based systems must sign in and provide information regarding their identity and the purpose of their visit.
- c) All visitors must be escorted to and from their destination.

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:

HIPAA Business Associate Contract and Other Arrangement Policy
HIPAA Personal Health Information Policy
HIPAA Security Compliance Policy
HIPAA Workforce Security Policy

Related Documents: