**Policy Title:** HIPAA Access Control

**Number:** TD-QMP-7018

**Subject:** Ensuring that access to EPHI is only available to those persons or programs that have been appropriately granted such access.

<table>
<thead>
<tr>
<th>Primary Department:</th>
<th>Secondary Department:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TennDent/Quality Monitoring/Improvement</td>
<td>TennDent/Administration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Effective Date of Policy:</th>
<th>Prior Policy or Cross Reference(s):</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/23/2011</td>
<td>10/1/2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Reviewed by TennDent Quality Monitoring/Improvement Committee:</th>
<th>Date Policy Last Revised:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Review Frequency:</th>
<th>Next Scheduled Review:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annually</td>
<td>7/1/2012</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TennDent Quality Monitoring/Improvement Committee Approval: OIn File</th>
<th>Approval Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9/23/2011</td>
</tr>
</tbody>
</table>

**Scope:**

TennDent staff, employees of Delta Dental of Tennessee (DDTN), TennDent/IT

**Purpose:**

TennDent is committed to conducting business in compliance with all applicable laws, regulations and TennDent policies. This Policy covers the unique user identification and password, emergency access, automatic logoff, encryption and decryption, firewall, and remote and wireless access procedures that will apply to electronic information systems that maintain Electronic Personal Health Information (EPHI) to assure that such systems are accessed only by those persons or software programs that have been granted access rights under the HIPAA Security Policy -- Information Access Management Policy.

**Authoritative Reference:**

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) HIPAA Security Rule [HIPAA Technical Safeguards] [see §164.312(a)(1) & (2)]

**Policy:**

1) Unique User Identification and Password
a. To uniquely identify and track each user for the purpose of access control to all networks, systems, and applications that contain EPHI, and the monitoring of access to the aforementioned networks, systems, and applications, TennDent must comply with the measures outlined in this Policy.

b. Any user that requires access to any network, system, or application that access, transmits, receives, or stores EPHI, must be provided with a unique user identification string.

c. When requesting access to any network, system, or application that accesses, transmits, receives, or stores EPHI, a user must supply his or her previously assigned unique user identification in conjunction with a secure password to gain access.

d. Each user’s password should meet the requirements as outlined in TennDents’ Password Best Practices Policy. Each user’s password must meet the following minimum requirements:

   • Passwords must be a minimum of eight characters in length
   • Passwords must not be words found in a Dictionary
   • Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc

e. If a system does not support the minimum structure and complexity as detailed in the aforementioned guidelines, one of the following procedures must be implemented:

   • The password assigned must be adequately complex to ensure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.
   • The legacy system must be upgraded to support the requirements of (letter d) as soon as administratively possible.
   • All EPHI must be removed and relocated to a system that supports the foregoing security password structure.

f. Users must not allow another user to use their unique user identification or password.

g. Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner.

h. Each user must ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications.

i. If a user believes their user identification has been compromised, they must report that security incident to their manager, who will contact the appropriate HIPAA Officer.

2) Emergency Access

   a. To ensure that access to critical EPHI is maintained during an emergency situation, each Department must establish and implement procedures to ensure that access to a system that contains EPHI and is used to provide treatment to an individual is made available to any
caregiver in the case of an emergency, if the denial or strict access to that EPHI could inhibit or negatively affect an individual’s care.

b. EPHI repositories that do not affect an individual’s care are not subject to the foregoing emergency access requirement.

3) Automatic Logoff
   a. Servers, workstations, or other computer systems containing EPHI repositories that have been classified as high risk must employ inactivity timers or automatic logoff mechanisms.
   b. The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity.
   c. Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms. (i.e., password protected screensaver that blacks out screen activity.) The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity.
   d. Applications and databases using EPHI, such as electronic claims records, must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 30 minutes of inactivity.
   e. Servers, workstations, or other computer systems that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.
   f. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
      • The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism.
      • The system must be moved into a secure environment.
      • All EPHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.
   g. When leaving a server, workstation, or other computer system unattended, Users must lock or activate the systems automatic logoff mechanism (e.g. CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing EPHI.

4) Encryption and Decryption
   a. Encryption of EPHI as an access control mechanism is not required unless the custodian of said EPHI deems the data to be highly critical or sensitive. Encryption of EPHI is required in some instances as a transmission control and integrity mechanism.

5) Firewall Use
   a. All networks housing EPHI repositories must be appropriately secured. To ensure that all networks that contain EPHI-based systems and applications are appropriately secured, each connection to outside the network must follow the steps outlined below.
b. Networks containing EPHI-based systems and applications must implement perimeter security and access control with a firewall.

c. Firewalls must be configured to support the following minimum requirements:
   • Limit network access to only authorized TennDent users and entities.
   • Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
   • Console and other management ports must be appropriately secured or disabled.
   • Implement mechanism to log failed access attempts.
   • Must be located in a physically secure environment.

d. TennDent must document its configuration of firewalls used to protect networks containing EPHI-based systems and applications. This documentation should include a configuration plan that outlines and explains the firewall rules.

e. The configuration of firewalls used to protect networks containing EPHI-based systems and applications must be submitted to and approved by the Information Security Officer.

6) Remote Access
   a. To ensure that all networks that contain EPHI based systems and applications are appropriately secured, each user must follow the remote access policies and procedures outlined below.

   b. Dialup connections (if allowed), directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.

   c. Authentication and encryption mechanisms are required for all remote access sessions to networks containing EPHI via an ISP (Internet service provider) or dialup connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and secured Citrix client access.

   d. The following security measures must be implemented for any remote access connection into a secure network containing EPHI:
      • Mechanisms to bypass authorized remote access mechanisms are strictly prohibited. For example, remote control software and applications, such as GoToMyPC.com, are not permitted.
      • Remote access workstations must employ a virus detection and protection mechanism.

   e. Users of remote workstations must comply with HIPAA Security Policy – Workstation Acceptable Use Policy.

   f. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.
g. Any user requesting remote access to a secure network containing EPHI-based systems and applications must be approved by the Security Officer to ensure that the remote workstation device being used by said user meets the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security. The owner of the secure network (IS or managing department) must ensure that the previous requirement has been satisfied before access is granted.

h. TennDent must establish a formal, documented procedure to ensure that remote workstations and mobile devices used by their users to remotely access secure networks containing EPHI-based systems and applications continue to meet the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security.

7) **Wireless Access**

a. To ensure that all networks that contain EPHI based systems and applications are appropriately secured, TennDent must follow the wireless access policies and procedures outlined below.

b. Wireless access to networks containing EPHI-based systems and applications is permitted so long as the following security measures have been implemented:
   - Encryption must be enabled.
   - MAC-based or User ID/Password authentication must be enabled. MAC-based (Media Access Control) authentication is based on a permitted list of hardware addresses that can access the wireless network. MAC addresses are hard coded on each network interface card and typically cannot be changed.
   - All console and other management interfaces have been appropriately secured or disabled.
   - Unmanaged, ad-hoc, or rogue wireless access points **ARE NOT PERMITTED** on any secure network containing EPHI-based systems and applications.
   - All wireless LANs do not utilize standard 2.4GHz, 5.0GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit EPHI may not allow encryption of that data stream. It has been determined that this is low risk because this implementation of infrared is very short distance and low power.
   - All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

c. Any user requesting access to a secure wireless network containing EPHI-based systems and applications must ensure that the wireless device being used by said user meets the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security. The owner (managing entity) of the secure wireless network must ensure that the previous requirement has been satisfied before access is granted.

d. TennDent must establish a formal, documented procedure to ensure that wireless devices used by their users to access secure networks containing EPHI-based systems and
applications continue to meet the security measures detailed in HIPAA Security Policy --

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 Device and Media Control Policy
HIPAA Device and Media Control Procedure
HIPAA Facility Access Controls Policy
HIPAA Information Access Management Policy
HIPAA Information Access Management Procedure
HIPAA Password Policy
HIPAA Periodic Evaluation of Security Policies and Procedures Policy
HIPAA Personal Health Information Policy
HIPAA Security Awareness and Training Policy
HIPAA Security Awareness Training Procedure
HIPAA Security Compliance Policy
HIPAA Security Verification and Validation Policy
HIPAA Server, Desktop and Wireless Computer System Policy
HIPAA System Security Procedure
HIPAA Workforce Security Policy
HIPAA Workforce Security Procedure

Related Documents: