**Procedure Title: HIPAA Risk Analysis Procedure**

**Number:** TD-QMP-P-7027

**Subject:** Risk Analysis

<table>
<thead>
<tr>
<th>Primary Department:</th>
<th>Secondary Department:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TennDent</td>
<td>HIPAA Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Effective Date of Procedure:</th>
<th>Prior Procedure 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>Date Procedure Last Reviewed:</th>
<th>Date Procedure Last Revised:</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/23/2011</td>
<td>7/1/2012</td>
</tr>
</tbody>
</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>Approvals:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TennDent Quality Monitoring Improvement Committee Approval: On File</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/23/2011</td>
</tr>
</tbody>
</table>

**Scope:**

This Risk Analysis Procedure is an eight-part process that TENNDENT will carry out step-by-step.

**Purpose:**

Risk is the likelihood that a specific threat will exploit certain vulnerability, and the resulting impact of that event. Risk analysis, is the starting point in an overall risk management process. It is a systematic and analytical approach that identifies and assesses risks and provides recommendations to reduce risk to an organization’s electronic protected health information (EPHI), and to allocate appropriate resources to reduce and correct potential losses.

**Procedure:**

<table>
<thead>
<tr>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
</table>
| IT Staff          | Determine what must be protected (assets) First copy the R:\Risk Assessment\HIPAA Risk Analysis (the previous year).mdb database to R:\Risk Assessment\HIPAA Risk Analysis (the current year).mdb database. Also copy the R:\Risk Assessment\ HIPAA Risk Analysis Threats (the previous year).xls to R:\Risk Assessment\ HIPAA Risk Analysis Threats (the
Begin the risk analysis process by reviewing the detailed inventory of EPHI produced from the Security Management Policy to ensure it is up to date. Conduct a detailed inventory of all computers, servers, routers and network devices. This is accomplished with the help of network scanning tool controlled by the database. The EPHI inventory and computer inventory used for the last execution of this procedure is contained in the database you copied above.

If the EPHI inventory and Computer Inventory are up to date continue the process.

<table>
<thead>
<tr>
<th>IT Staff</th>
<th>Threat Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify all potential threats to EPHI and related information systems. A threat is defined as “something or someone that can intentionally or accidentally exploit vulnerability.”</td>
<td></td>
</tr>
</tbody>
</table>

In general there are three types of threats:

- **Natural**: Floods, earthquakes, tornados, etc.
- **Human**: Unintentional (incorrect data entry or accidental deletion of data) and intentional (denial of service attack),
- **Environmental**: Power failures, hazardous material spill, etc.

The threats or vulnerabilities used for the last execution of this procedure are contained in R:\Risk Assessment\HIPAA Risk Analysis Threats (the current year).xls file and can be used for a starting point, making sure to include any additional threats that have been identified.

<table>
<thead>
<tr>
<th>IT Staff</th>
<th>Vulnerability Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify the vulnerabilities of EPHI and related information systems. Vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that can be exploited by a threat and result in misuse or abuse of EPHI.</td>
<td></td>
</tr>
</tbody>
</table>

A. Review vulnerability sources.
B. Perform security assessments.

Vulnerability sources include system and data owner questionnaires, on-site review of information systems, audit reports, and information system test and evaluation reports. Vulnerability lists such as the NIST vulnerability database (http://icat.nist.gov) and Bugtraq, as well as advisories from security vendors and security organization such as CERT are also good tools.

The threats or vulnerabilities used for the last execution of this procedure are contained in R:\Risk Assessment\HIPAA Risk Analysis Threats (the current year).xls.
current year).xls file and can be used for a starting point, making sure to include any additional vulnerability that have been identified.

<table>
<thead>
<tr>
<th>IT Staff</th>
<th>4. Security Control Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Analyze the security controls that have been implemented or will be implemented to protect EPHI; this includes both preventive and detective controls.</td>
</tr>
</tbody>
</table>

The preventive security controls are designed to prevent or restrict the exploitation of vulnerabilities (e.g., access control, authentication). Detective controls detect and report when violations occur (e.g., audit trail, alarm). The analysis should clearly define what security controls are being used to protect specific EPHI, how they’re being used, and any gaps between how they’re being used and how they’re supposed to be used.

Using Appendix A in this document determine if additional questions or information needs to be included from the system questionnaires considering any additional risks or vulnerabilities produced in steps 2, 3 and 4 above. If additional information is needed change the database before producing the questionnaires.

Using the questionnaires/checklists produced by the database distribute and assign responsibility to those persons who must complete the questionnaires.

<table>
<thead>
<tr>
<th>IT Staff</th>
<th>Risk Likelihood Determination</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Assign risks ratings that indicate the probability that vulnerability will be exploited by a particular threat. Three factors should be considered: 1) Threat motivation and capability. 2) Type of vulnerability. 3) Existence and effectiveness of security controls.</td>
</tr>
</tbody>
</table>

Suggested levels to use:

Likelihood Definition

High Threat is highly capable, motivated, or likely and current security controls are ineffective.

Medium Threat is capable, motivated or likely, but there are security controls in place that may prevent exploitation of specific vulnerabilities.

Low Threat is not capable, motivated or likely or current security controls will likely prevent exploitation specific vulnerabilities.

<table>
<thead>
<tr>
<th>IT Staff</th>
<th>Impact Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Determine the impact that would result if a threat were to successful</td>
</tr>
</tbody>
</table>
**Procedure: HIPAA Risk Analysis**

Information system and EPHI owners should be interviewed to determine the impact in the following areas:

- **Confidentiality**: EPHI is disclosed or accessed in an unauthorized manner.
- **Integrity**: EPHI is improperly modified.
- **Availability**: EPHI is unavailable to authorized users.

The Impact Level is High, Medium or Low as defined in the Security Management Policy and assigned to the EPHI repository.

## IT Staff

**Policies**

A. The review and analysis of the existing policies and procedures is done to gauge the compliance level within the organization. Policies define acceptable use, provide consistency and are used to lower risk levels to acceptable levels.

Policies need to be reviewed periodically to keep them up to date. They provide a paper trail in cases of due diligence. It is essential that policies be structured in a way that they are as light as possible, without missing any important issues:

- a. Simple and practical
- b. Easy to manage and maintain
- c. Easy to access by people seeking specific information

B. Password policies are necessary to protect the confidentiality of information and the integrity of systems by keeping unauthorized users out of computer systems. Inadequate password policies or lax enforcement of password policies can lead to problems and increase risk.

A questionnaire for each detail record of the inventory of computers, servers, routers and network devices should be filled out and signed by the respondent. In Appendix A is a list of the current questions.

**Analysis of acceptable risks**

One of the final tasks is to assess whether or not the existing policies, procedures and protection items in place are adequate. If there are no safeguards in place providing adequate protection, it can be assumed that there are vulnerabilities. A review of the existing and planned safeguards should be performed to determine if the previously known and discovered risks and threats have been mitigated.

## IT Staff

Use the information obtained in the above steps to identify the level of risk to specific EPHI and related information systems. For each vulnerability and associated possible threat, make a risk determination based on:

- The likelihood a certain threat will attempt to exploit a specific
vulnerability. The level of impact should the threat successfully exploit the vulnerability. The adequacy of planned or existing security controls.

Risk Levels to use:

Risk Level Required Action

High Security controls should be implemented or improved as quickly as possible. Medium Security controls should be implemented or improved in a reasonable amount of time. Low Existing security controls are likely adequate or the risk is acceptable.

IT Staff Security Control Recommendations

Using all of the above information, conclude the Risk Analysis process by proposing security controls that can mitigate or eliminate the identified unacceptable risks to EPHI. These controls should reduce the level of risk to EPHI and related information systems to an acceptable level and will be documented in the Risk Analysis Report. These proposed controls would then be evaluated when the process moves to risk mitigation.

A balance must be found between too much security (very restrictive use, high cost) and too little security (unrestricted use, low visible cost, but high danger). It is important that the value of the information and processes in the system is determined, and the risks identified, so that appropriate countermeasures can be implemented.

There are three basic responses to a risk, once you have identified and defined it. The first is to accept the risk and work on other things. This is often the best approach for very low risks or ones about which TENNDENT cannot effectively do anything. The second is to try to mitigate the risk. This means trying to reduce the risk by reducing the potential impact, reducing the likelihood that it will affect TENNDENT, or both. For example, we apply patches our server, thus reducing the likelihood that the new virus will affect us. The third is to try to transfer the risk. This means that we would get someone else to accept at least some of the risk for us. For example, we would buy insurance.

IT Staff Conclusion

In summary the threat and risk assessment process is not a means to an end. It is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organization in terms of integrity, availability and confidentiality. The threat and risk assessment should be an integral part of the overall life cycle of TENNDENT. Organizations that do not perform a threat and risk analysis are leaving themselves open to
situations that could disrupt, damage or destroy their ability to conduct business. Therefore the importance of performing a threat and risk analysis must be realized by both the staff supporting the infrastructure and those that rely upon it for their business.

Appendix A

System Risk Analysis Checklist

1. Workstation Computer
   a. Is the admin group restricted in membership?
   b. Is an actual login required?
   c. Are there individual usernames for all employees using this system?
   d. Is password strength appropriate?
   e. Is EPHI stored on this system?
   f. Is Sensitive Information stored on this system?
   g. Is a firewall configured?
   h. Is an antivirus program installed and properly configured?
   i. Are the latest virus definitions installed?
   j. Is this system backed up?
   k. Is a password protected screensaver configured?
   l. Is the Guest account disabled?
   m. Is the system currently patched to appropriate levels?
   n. Is the system set for Automatic Updates and set to ask the user if he/she wishes to install updates?
   o. Are there single points of failure for any services (If this system goes down will it adversely affect TENNDENT)?
   p. Are workstation monitors in public areas positioned in a way to avoid observation by visitors?
q. Is the user allowed to install software on this machine?

r. Is the user allowed to use media (CD, USB Key, Floppy etc.) brought from home?

s. Is the user allowed to connect portable devices to this machine?

2. Server

a. Is the system backed up regularly?

b. Is the back process tested by restoring information to a temporary location?

c. Is the admin group restricted in membership?

d. Is an actual login required?

e. Are there individual usernames for all employees?

f. Is password strength appropriate?

g. Is EPHI stored on this system?

h. Is Sensitive Information stored on this system?

i. Is a firewall configured?

j. Is an antivirus program installed and properly configured?

k. Are the latest virus definitions installed?

l. Is the server connected to a UPS?

m. Are there open ports to the public network? (Http, FTP or other.)

n. Is a password protected screensaver configured?

o. Is the Guest account disabled?

p. Is the Administrator account renamed?

q. Is the system currently patched to appropriate levels?

r. Is the system set for Automatic Updates and to ask the user if he/she wishes to install updates?

s. Has the everyone group been removed from network shares and been replaced with TENNDENT-All where appropriate?
t. Are there single points of failure for any services (If this system goes down will it adversely affect TENNDENT)?

u. Is Internet Information Server (IIS) running on this system?

v. Has the IIS Lockdown Tool been run on this server?

w. Is the server in a secure location (Locked room with authorized access only)?

3. Firewall

a. Has the administrator password been changed?

b. Are ICMP ping requests blocked?

c. Is Remote Management disabled?

d. Is Remote Upgrade disabled?

e. Is Network Address Translation (NAT) enabled?

f. Is IP address filtering enabled and functioning?

g. Is IP service filtering enabled and functioning?

h. Is MAC address filtering enabled and working?

i. Is Virtual Server disabled?

j. Are unwanted ports shut down to keep them from serving as a starting point of an attack?

k. Is logging configured and working?

l. Is the appliance plugged into a UPS?

m. Is the firewall set to default Deny all connections from the Internet to the LAN by default?

n. Are there single points of failure for any services (If this system goes down will it adversely affect TENNDENT)?

o. Is the configuration backed up on another system regularly?

p. Is the configuration backup encrypted?

q. Is the firewall in a secure location (Locked room with authorized access only)?

4. Routers
a. Has the administrator password been changed?
b. Are ICMP ping requests blocked?
c. Is Remote Management disabled?
d. Is Remote Upgrade disabled?
e. Is Network Address Translation (NAT) enabled?
f. Is IP address filtering enabled and functioning?
g. Is IP service filtering enabled and functioning?
h. Is MAC address filtering enabled and working?
i. Is Virtual Server disabled?
j. Are unwanted ports shut down to keep them from serving as a starting point of an attack?
k. Is logging configured and working?
l. Is the appliance plugged into a UPS?
m. Is the configuration backed up to another location regularly?
n. Is the configuration backup encrypted?
o. Is the router in a secure location (Locked room with authorized access only)?

5. Wireless Routers
a. Has the administrator password been changed?
b. Are ICMP ping requests blocked?
c. Is Remote Management disabled?
d. Is Remote Upgrade disabled?
e. Is Network Address Translation (NAT) enabled?
f. Is IP address filtering enabled and functioning?
g. Is IP service filtering enabled and functioning?
h. Is MAC address filtering enabled and working?
i. Is Virtual Server disabled?
j. Are unwanted ports shut down to keep them from serving as a starting point of an attack?

k. Is logging configured and working?

l. Is the appliance plugged into a UPS?

m. Is the configuration backed up to another location regularly?

n. Is the configuration backup encrypted?

o. Has the wireless SSID been changed from “default”?

p. Has the wireless channel been changed from the default value?

q. Is the 128-bit WEP (Wired Equivalent Privacy) protocol enabled?

r. Is the wireless router in a secure location (Locked room with authorized access only)?

6. VPN Server

a. Has the administrator password been changed?

b. Are ICMP ping requests blocked?

c. Is Remote Management disabled?

d. Is Remote Upgrade disabled?

e. Is Network Address Translation (NAT) enabled?

f. Is IP address filtering enabled and functioning?

g. Is IP service filtering enabled and functioning?

h. Is MAC address filtering enabled and working?

i. Is Virtual Server disabled?

j. Are unwanted ports shut down to keep them from serving as a starting point of an attack?

k. Is logging configured and working?

l. Is the appliance plugged into a UPS?

m. Is an actual login required?

n. Are there individual usernames for all employees using this system?

o. Is user password strength appropriate?
p. Is the configuration backed up to another location regularly?

q. Is the configuration backup encrypted?

r. Is the VPN server in a secure location (Locked room with authorized access only)?

Related Policies and Procedures: