Summary
This document outlines the recommended steps for using the Privacy and Security toolkit provided by the Regional Extension Center (REC). The documents/tools listed below are provided to you on CD, through email, within an online portal and/or in paper format. Please contact your REC if you have any questions or need any assistance working with these documents.

Instructions
It is recommended to start with number 1, Meaningful Use Fact Sheet, and then continue working through each step one at a time. Some items may require additional assistance from your IT resources, EHR vendor, as well as your REC. The Office Manager, Physician, and/or the most knowledgeable security expert on staff would be the best person(s) to follow this checklist.

A. Meaningful Use and Cybersecurity Guide
   ____ 1. Meaningful Use Fact Sheet
   The Privacy and Security Meaningful Use Fact Sheet will help prepare your Practice for stage 1 Meaningful Use criteria regarding Privacy and Security. Please review this document first.

   ____ 2. Cybersecurity Guide
   This best practices guide can help your Practice validate that you are meeting the basic privacy and security requirements which are outlined in each of ten sections. Please complete the checklists at the end of guide and return them to your REC.

B. Privacy and Security Gap Analysis
   ____ 3. EHR Security Assessment
   This assessment checklist helps ensure that EHR security settings are properly configured to industry best practices. Please complete and return the checklist to your REC.

   ____ 4. Privacy and Security Checklist with Guidance Instructions
   The privacy and security checklist is a great tool for performing a gap analysis for HIPAA and HITECH. Once completed and returned, your REC can better understand your needs and can better assist you.
C. Policies and Procedures

5. Policies and Procedure Templates
Your REC has provided policy and procedure templates either on a CD, through email, and/or online which can be customized to meet the needs of your Practice. For any large templates, an instructional document has been provided to help your Practice better understand which areas need filled in and updated.

D. Security Awareness and Training

6. Security Awareness PowerPoint Training
Your REC has provided PowerPoint training either on CD, through email, and/or online which can provide training to all staff within the Practice. There are separate PowerPoints for Admin Staff and End Users which could provide regular security awareness and training for the Practice.

E. Guidance Documents

7. Guidance Documents
Guidance documents are a great way to learn privacy and security best practices, technologies, and to obtain information about regulatory requirements. Your REC has created guidance documents that include:

- Backup & Recovery
- Breach Notification
- Red Flags Rule
- Wireless Networks

F. Risk Analysis/Assessment

8. HIT Security Risk Assessment Questionnaire
The attached Do It Yourself (DIY) Risk Assessment Tool has been provided to the tnREC by the ONC for the purpose of identifying risks to ePHI and identifying steps to take to mitigate those identified risks. The tool is pre-populated with risks typically identified in organizations similar to yours. Completion of this tool, in and of itself, does not guarantee that an organization will meet the measure of success of the privacy and security objective required for Meaningful Use. It does, however, provide a foundation for meeting the measure of success and starting a Risk Analysis and Risk Management program as required pursuant to the HIPAA Security Rule.