Meaningful Use Security Analysis Workbook & Documentation

Disclaimer

The Security Risk Analysis Worksheet is provided for informational purposes only. Use of this worksheet is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations. This worksheet is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights Health Information Privacy website. Also: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Definition of Terms:

EHPI: Electronic Protected Health Information

Required: Similar to a standard in that a covered entity must comply with it

Addressable: An assessment must be performed to determine whether the specification is a reasonable and appropriate safeguard in the covered entity's environment.
Addressable Decision: After performing the assessment a covered entity decides if it will implement the addressable implementation specification, implement an equivalent alternative measure that allows for measure compliance, or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment.
Addressable items must have the assessment and decision documented.

Scope of this Risk Analysis

The scope of the following risk analysis includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that our organization creates, receives, maintains, or transmits. This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. This analysis takes into account all of our e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of our e-PHI.

Data Collection

Through this document we have identified where the e-PHI is stored, received, maintained or transmitted and documented our information gathering methods.

Identification and Documentation of Potential Threats and Vulnerabilities

Through this workbook our organizations has identified and documented reasonably anticipated threats to e-PHI.

If applicable we have identified and documented vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.

Determining the Potential Impact of Threat Occurrence

Through this document we have considered the "criticality," or impact, of potential risks to the confidentiality, integrity, and availability of e-PHI. We have assessed the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability.
In this workbook we have documented all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the
confidentiality, availability and integrity of e-PHI within our organization.

Determining the Level of Risk

Where appropriate we have assigned risk levels for all threat and vulnerability combinations identified during this risk analysis. Where appropriate we have assigned a risk level of low, medium or high based on the likelihood and impact levels.

1) Risk Analysis (REQUIRED): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity.

- □ Identify the EPHI within your organization (This includes EPHI that you create, receive, maintain, or transmit. The EPHI can reside on workstation, servers, laptops, PDA's, tablets, etc.)
  - ➢ List the EPHI that you have identified within your organization
  - ➢ What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
  - ➢ What are the human, natural, and environmental threats to information systems that contain e-PHI?

____

____

____

____

____

____

2) Risk Management (REQUIRED): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

- □ Identify security measures that are already in place to protect EPHI (This can be a comprehensive view of all measures, whether administrative, physical or technical, such as an over-arching security policy; door locks to rooms where EPHI is stored, or the use of password-protected files.)

- ➢ List security measures that are already in place to protect EPHI:

____

____

____

____

____

____

3) Sanction Policy (REQUIRED): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

□ Develop, apply, and implement policies specific to violations of the security policies and procedures

- ➢ List your violation policies:

____

____

____

____

____

____

□ Make sure policies developed, applied, and implemented above provide appropriate sanctions for workforce members who fail to comply with your security policies and procedures

□ Include your sanction policy in your workforce manual and train your staff on the policy

4) Authorization and/or Supervision (ADDRESSABLE): Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.

□ Make sure the procedures used by your workforce are consistent with your access policies

□ People who should have access actually have that access

□ People who should not have access are actually prevented from accessing the information

Assessment Notes and Conclusion: ____

____

____

____

____

____

____

Decision: ____

____

____

____

____

____

____

5) Password Management (ADDRESSABLE): Implement procedures for creating, changing, and safeguarding passwords.

□ Make sure your workforce training includes topics such as not sharing passwords with other workforce members or not writing down passwords and leaving them in open areas

Assessment Notes and Conclusion: ____

____

____

____

____

____

____

Decision: ____

____

____

____

____

____

____

6) Data Backup Plan (REQUIRED): Establish and implement procedures to create and maintain retrievable exact copies of EPHI.

□ Make sure your procedures identify all sources of EPHI that must be backed up such as patient accounting systems, electronic medical or health records, digital recordings of diagnostic images, electronic test results, or any other electronic documents create or used that contain EPHI

➢ List your sources of EPHI that must be backed up:

____

____

____

____

____

____

7) Written Contract or Other Arrangements (REQUIRED): Document the satisfactory assurances required by this section through a written contract or other arrangement with the business associate that meets the applicable requirements.

□ Make sure you have contracts in place with outside entities entrusted with health information generated by your office

➢ List outside entities entrusted with health information generated by your office:

____

____

____

____

____

____

□ Make sure the contracts provide assurances that the information will be properly safeguarded

8) Facility Security Plan (ADDRESSABLE): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

□ Make sure your office policies and procedures identify controls to prevent unauthorized physical access, tampering, and theft of EPHI (i.e. locked doors, signs warning of restricted areas, surveillance cameras, alarms, and identification numbers and security cables on computers)

- ➢ List controls to prevent unauthorized physical access, tampering, and theft of EPHI

____

____

____

____

____

____

Assessment Notes and Conclusion: ____

____

____

____

____

____

____

Decision: ____

____

____

____

____

____

____

9) Maintenance Records (ADDRESSABLE): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (i.e. hardware, walls, doors, locks, etc.).

□ Make sure policies and procedures are implemented that specify how repairs and modifications to a building or facility will be documented to demonstrate that the EPHI is protected

- ➢ List how building or facilities repairs and modifications will be documented to demonstrate that the EPHI is protected

____

____

____

____

____

____

Assessment Notes and Conclusion: ____

____

____

____

____

____

____

Decision: ____

____

____

____

____

____

____

10) Workstation Use (Required):

- □ Make sure your office policies and procedures specify the use of additional security measures to protect workstations with EPHI, such as the use of privacy screens, enabling password protected screen savers, or logging off the workstation.
  - ➢ List your offices additional security measures to protect workstations with EPHI:

____

____

____

____

____

____

11) Disposal (Required): Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.

- □ Make sure your office has a method of destroying EPHI on equipment and media you are no longer using (i.e. hardware erasure software)
  - ➢ List your offices method of destroying EPHI on equipment and media no longer in use:

____

____

12) Database Backup and Storage (Required): Create a retrievable, exact copy of EPHI, when needed, before movement of equipment

- □ Make sure your office has a process in place to create a retrievable, exact copy of EPHI before the equipment on which it is stored is moved
  - ➢ List your process here:

____

____

13) Unique User Identification (Required): Assign a unique name and/or number for identifying and tracking user identity

- □ Make sure each user of your system in your office is assigned a unique user identifier that is used to track user activity within information systems that contain EPHI

14) Automatic Logoff (Addressable): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity

- □ Make sure your current information systems have an automatic logoff capability to ensure that unauthorized users do not access data on unattended workstations (Practice Director does have an activity timeout feature in versions 4.0 and higher)

- □ Make sure you have enabled and configured the automatic logoff capability of your current information systems to ensure that unauthorized users do not access data on unattended workstations (You can enable and configure the inactivity timeout of Practice Director by going to the Administration menu > Inactivity Timeout)

Assessment Notes and Conclusion: ____

____

____

____

____

____

____

Decision: ____

____

____

____

____

____

____

15) Person or Entity Authentication (Required): Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed

□ Make sure your system requires the input of something known only to the person or entity seeking access to EPHI (i.e. a password or PIN) prior to granting the requested access

□ Make sure each person or entity seeking access to EPHI has their own password known only to that individual prior to granting access to the system

16) Encryption (Addressable): Implement a mechanism to encrypt EPHI whenever deemed appropriate

□ Based on your required risk analysis, decide if encryption is needed to protect the transmission of EPHI between your office and outside organizations. If not, make sure measures are in place that ensure the protection of this information (i.e. password protection of documents or files containing EPHI and/or prohibiting the transmission of EPHI via email)

Assessment Notes and Conclusion: ____

____

____

____

____

____

____

Decision: ____

____

____

____

____

17) Other:

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

Signatures, Periodic Review and Updates to this Risk Assessment

This risk analysis process is ongoing. We conduct continuous risk analysis to identify when updates are needed. Regardless of the fact that the Security Rule does not specify how frequently we perform risk analysis, we as part of our comprehensive risk management process are continuously cognizant of security risk factors and continuously as they arise take mitigating action.

Organization Name :____

Completed/Reviewed By: ____________________________________

Completed Date :____________________________

Signature: ___________________________________

Reviewed Date: _____________________________

Signature: ___________________________________

Reviewed Date: _____________________________

Signature: ___________________________________

Reviewed Date: _____________________________

Signature: ___________________________________