HIPAA Security Rule
Risk Analysis Checklist

General Instructions: The purpose of this checklist is to provide guidance to covered entities on how to perform a basis risk analysis as mandated by the HIPAA security rule. It is not intended to be a comprehensive listing of all possible threats, risk factors, and safeguards. (A more extensive risk analysis may be necessary depending on the types of EPHI present at your facility and the frequency of its use.) To perform a basis risk analysis using this checklist, complete each section and retain at least one copy of this document for up to six years as required by the security rule. Note that each section includes its own instructions.

Section I: Inventory of Electronic Protected Health Information

Instructions – Identify the types of personally identifiable information that are maintained, stored, or transmitted via computer networks or workstations at your place of business. Items in the listing below that are marked with a "+" symbol may require specific security attention.

- ❑ Name
- ❑ Social security number
- ❑ Address
- ❑ Date of birth (+)
- ❑ Medical record number (+)
- ❑ Hospital admission date (+)
- ❑ Hospital discharge date (+)
- ❑ Date of death
- ❑ Member or account number (+)
- ❑ All ages over 89
- ❑ Relatives' names
- ❑ Any vehicle/other device serial number
- ❑ Health plan beneficiary numbers (+)
- ❑ Certificate/license number
- ❑ Account numbers
- ❑ Telephone/fax numbers
- ❑ Voice/fingerprints
- ❑ Photos
- ❑ Full-faced photographic images
- ❑ Email addresses
- ❑ IP address (web URL)
- ❑ Any other unique identifying number, characteristic, or code
- ❑ Pre-existing medical condition (+)
- ❑ Drug test results (+)
- ❑ Fitness-for-duty test results (+)
- ❑ Physician certifications (+)
- ❑ Reports of injuries or illnesses (+)
- ❑ Any other record relating to an individual's health status (+)

Section II. Location of EPHI and Other Electronic Personally Identifiable Information

Instructions – Identify the physical location of any information specified above. This step will help you determine the types of controls that must be implemented in compliance with the security regulation.

- ❑ Computer workstations
- ❑ Computer networks
- ❑ Email servers
- ❑ Fax servers
- ❑ Back-up systems
- ❑ Back-up media

Section III. Internal and External Security Threat Assessment

Instructions - Identify potential threats and assess the risk level associated with each threat. Use the "Other" option to identify threats not included in each listing. Threat assessments (low, moderate, high, very high) should consider prior incidents and the current likelihood of an incident occurring or repeating.

	Low	Moderate	High	Very High
Natural Threats				
Floods	❑	❑	❑	❑
Earthquakes	❑	❑	❑	❑
Tornados	❑	❑	❑	❑
Hurricanes	❑	❑	❑	❑
Other: _____	❑	❑	❑	❑

	Low	Moderate	High	Very High
Human Threats:				
Unauthorized access	❑	❑	❑	❑
Installation of malicious software	❑	❑	❑	❑
Accidental deletion of data	❑	❑	❑	❑
Accidental transmission of data	❑	❑	❑	❑
Theft of back-up media	❑	❑	❑	❑
Theft of workstations	❑	❑	❑	❑
Data entry errors	❑	❑	❑	❑
Other: _____				
Environmental Threats:				
Fires	❑	❑	❑	❑
Explosions	❑	❑	❑	❑
Power failures	❑	❑	❑	❑
Hazardous material spills	❑	❑	❑	❑
Other_____	❑	❑	❑	❑

Section IV: Inventory of Existing Security Controls

Instructions – Identify existing security controls by placing a checkmark next to each existing item in the list below. Controls that have not been implemented may need to be adopted to ensure compliance with the security rule. Note: This is not a complete listing of all available, required, or addressable controls. As such, space has been provided to identify other existing safeguards. Refer to the complete text of the security rule for complete requirements.

- ❑ Unique user log-in processes
- ❑ Password requirements for system and network access
- ❑ Procedures to terminate passwords for separated employees
- ❑ Firewalls
- ❑ Procedures to report and document security incidents
- ❑ Anti-virus software
- ❑ Contingency plans / disaster recovery plans
- ❑ Data encryption
- ❑ Workstation monitoring
- ❑ System backups
- ❑ Offsite storage of backup media
- ❑ Storage of backup media in fireproof safe
- ❑ Storage of backup media in locked cabinet
- ❑ System security levels assigned based on business need
- ❑ Other: _____

Form Completed By:

_____ _____

Signature of Designated Security Official or HR / IT Manager

Date

