Policy No. 1
Security Management Policy and Procedure

Policy:

The purpose of this policy is to establish the process to identify the risks to the practice and to manage the risks.

1. Risk Analysis

The practice will conduct a survey of all computer and information systems in order to determine where electronic protected health information is stored, how it is transmitted, and which employees currently have access. The practice will also identify the type of information contained on each system and the impact to daily activities that would be caused by a loss of this information. This process will be repeated for all new equipment, information systems or computer systems that are installed.

The practice will use good faith efforts to identify all known and/or anticipated threats to electronic protected health information and any vulnerability that would cause a program or system to be impacted by threats.

2. Risk Management

When risks are identified, the practice's Security Officer will be responsible for overseeing that the costs associated with minimizing the risks are identified.

It will be the responsibility of the practice's Security Officer to gather information and present this information to the appropriate decision-making authorities within the practice so that determinations can be made based upon the risks to the practice and the costs associated with mitigating these risks.

3. Employee Sanctions

Employees will be sanctioned appropriately for breaching security policies and procedures in accordance with the practice's general disciplinary policies, and will take into account the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicates a pattern or practice of improper use or disclosure of protected health information.

4. Information System Activity Review

The practice will determine which reports the practice's information systems and software programs are capable of generating, including, but not limited to audit logs, access reports, and security incident tracking reports.

The practice will run such reports at intervals as determined by the practice's Security Officer based upon the usefulness of the report.

Procedure:

1. The practice's Security Officer will be responsible for overseeing the completion of Worksheet #1 and updating the Worksheet as new systems or software programs are added.
2. The practice's Security Officer will oversee completion of Worksheets #2 and #3. These Worksheets should be updated at least yearly or any time that a new threat or vulnerability is identified or any time that a new system or software program is added.
3. The practice's Security Officer will be responsible for conferring with administrative personnel who have authority to make decisions with respect to which security solutions may be implemented (based upon a cost/benefit analysis).
4. Employees who do not adhere to HIPAA Policies, including Security Policies will be appropriately disciplined.
5. The practice's Security Officer will be responsible for listing all reports and the frequency with which each should be run routinely, as well as any events that will trigger the running of the report.
6. The practice's Security Officer will be responsible for setting a schedule for running and reviewing reports and for maintaining all reports for a period of six years.
7. If the practice's Security Officer identifies suspicious activity based upon the reports, it will be investigated and the results of such investigation documented.

Risk Analysis Worksheet #1 –
Identification of All Software Programs/Information Systems/Databases

List all Software Programs/ Information Systems/Databases that are used within your office	Description	Is it used to maintain or transmit electronic protected health information?	Which computers have this program/system/ database installed?

Worksheet #2

In the attached grid, list all threats to your information systems, including threats falling within all of the categories listed below. Include all threats that have occurred in the past and threats that you think could potentially impact your information systems that house electronic protected health information.

I. Human Threats

Internal Human Threats – Unintentional

List any threats to your information systems based upon unintentional internal human threats. This would include damage by your employees or other workforce that are unintentional. (Examples: employees inadvertently losing passwords or disclosing passwords to unauthorized users, employees downloading information from the internet or receiving e-mails that may contain viruses).

Internal Human Threats - Intentional

List any threats to your information systems based upon intentional internal human threats. This would include threats to information systems by your employees or other workforce that are intentional. (Examples: attempts to gain unauthorized access, such as password guessing or sharing; intentional acts of sabotage by disgruntled employees, such as intentionally sending viruses or intentionally corrupting a database).

External Human Threats

List any threats to your information systems based upon external human threats. This would include threats to information systems by persons who are not current employees or workforce. (Examples: attempts to gain unauthorized access; computer hackers; intentional acts of sabotage by disgruntled former employees, such as sending viruses to your computer system, etc.; or attempts to gain access by former employees who have current passwords).

II. Natural Threats

List any threats to your information systems based upon natural threats. This would include threats to information systems from natural causes. (Examples: floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and hurricanes).

III. Environmental Threats

List any threats to your information systems based upon the environment where your information systems are located. (Examples: power outages, pollution, chemical exposure, and liquid leakage (such as a water pipe leak or break)).

Threat Worksheet: Grid

Describe threat in the space provided below:	Has threat occurred in the past? (yes or no)	Likelihood of threat occurrence? (low, medium, or high)	Would the occurrence of this threat impact confidentiality of data? (yes or no)	Would the occurrence of this threat impact integrity or availability of data? (yes or no)

Risk Analysis Worksheet #3

(Copy this form before completing – you will want to complete a separate worksheet for each information system that is used within the organization to store electronic protected health information or to transmit electronic protected health information- attach a separate sheet of paper for additional space needed)

Describe system identified in Worksheet #1 by name or function: (examples: lab reporting system, operating system, data repository, electronic medical record, patient scheduling system, e-mail system):

Describe the data and information that is contained in or transmitted by this system (example, lab results, progress notes, radiology results, etc.):

How would daily operations be impacted if this system was unavailable or the data was lost?

Who uses this system (list by name or job title/category)?

Who has access to the system to provide support to the system (include employees and non-employees, such as vendor representatives)?

Describe the hardware that is used to run this system (include hardware that houses the database, such as a mainframe computer) (for example, is the system housed on one PC, is it on a main frame computer with "dumb terminals", is it the database housed on a server and accessed with PCs?):

Describe the software that is used to run this system (For example, list the name of the vendor's software and including any operating systems that are required to run the system – such as Microsoft Windows and the particular version of Microsoft Windows):

List any interfaces with other systems (for example, a lab system may have an interface with a clinical data repository or an electronic medical records system, so that the data can be shared between the two systems):

Do you have documentation to support the use of this program or information system (if so, this information should be located and kept in a place that is easily accessible by the Security Officer?)?

Are there currently any written policies that govern how this system is used? If so, describe or list below:

How is the information contained on this system backed up and how often is backup completed?

Do you feel comfortable that the information contained on this system could be retrieved from the backup if it was lost (either by your own personnel or through a vendor/IT consultant)? (Describe why or why not.)

How long would it take to retrieve the information from the backup if necessary?

Review the Threat Worksheet and Grid (Complete the Worksheet and Grid at this time if you have not already done so). Is there anything about this system that makes it vulnerable to the threats set forth in the grid (for example, lack of firewall would make system more vulnerable to external human threats)?

Was this particular system vulnerable to any threats in the past? Describe:

If the answer above was "yes", what was done to prevent the reoccurrence of the threat?

Talk to the vendor who sold you this system or software or talk to your IT support personnel and ask if there are any patches that are needed for your particular software or upgrades to correct any vulnerabilities known by the vendor (alternatively you may be able to look this information up on the internet on the vendor's website). List any steps or patches that were recommended by the vendor, IT personnel or consultants and include the cost, if applicable:

_____

_____

_____

_____