[Name of organization]

HIPAA Privacy and Security Policy and Procedures

I. Assignment of HIPAA Privacy/Security Officer

_____ has been designated as our HIPAA Officer by _____ and has authority to establish, implement, and enforce these policies and procedures for the security and privacy of our patients protected health information (PHI).

II. Risk Assessment

HIPAA Officer is responsible for conducting annual HIPAA privacy and security risk assessment. The assessment will be completed with the assistance of at least two other employees.

Additional risk assessments may be necessary each time (1) new software or hardware is acquired and placed in service; (2) when a new service or procedure is initiated; (3) when there is a significant change in an existing service or procedure; or (4) when there is a change or addition to the physical layout of our office.

The HIPAA Officer will periodically but at least quarterly review the DHHS's HIPAA website to determine if there have been any changes in the HIPAA rules and regulations and to determine if any changes or modifications to this policy and procedure is necessary due to changes in HIPAA rules, regulations or regulatory interpretations.

[See Addendum IV for sample risk assessment form]

III. Policy regarding physical access to building

(Explain how entrance to office is controlled. The following is an example—modify or re-write as needed for your facility.)

Employees access our office via main entrance or employee entrance. Main entrance is locked after hours and is unlocked each morning at 8:00. The Office Manager has the key to both entrances and is responsible for

unlocking main entrance each AM. Employee entrance is accessed only via key. Employees or service personal may gain entrance through the employee entrance by knocking on the door.

IV. Policy regarding confidentiality of all forms of PHI

All PHI regardless of its form, mechanism of transmission, or storage is to be kept confidential. Only individuals with a business need to know are allowed to view, read, or discuss any part of a patient's PHI. During initial new hire orientation and at annual HIPAA training employees are reminded that any viewing, reading, or discussions of PHI that is not for business purposes is prohibited. An employee who violates this confidentiality policy will be subject to sanctions up to immediate termination. All employees are required to verify in writing that they have read and will comply with our policy regarding confidentiality of all forms of PHI.

V. Policy regarding Security of electronic PHI (e-PHI)

Employees whose job functions require access to our computer system will be given a secure, unique password to access the system. Passwords will consist of at least five characters, upper and lower case, alpha numeric and shall be changed at least every 90 days.

Access will be immediately terminated for employees who leave our employment. [Include reference to APRNs, PAs, CRNAs, and employed MDs etc.]

All PHI transmitted to third parties will be transmitted on secured lines. The security of transmission lines will be verified via contract with third party responsible for transmitting our patient's PHI.

No digitally stored PHI shall leave this facility without being first encrypted; this includes laptops, flash drive devices, CDs, and e-mail.

VI. Patient request for accounting of all disclosures made by (Your facility)

Patients have a right to request an accounting of all disclosures of their PHI made by (name of your facility). When a patient makes such a request, (name of responsible employee) will be notified. The patient will be told when the information will be available and given the option of waiting or returning to pick-up the data.

VII. Patient request for restriction of PHI paid for "out of pocket"

Patients who pay for a procedure, test, or service out of pocket (fully paid for by patient with no reimbursement or additional payment by a third party), have a right to have all information regarding such procedure/test held confidentially and not released to third parties. To exercise this right the patient must (1) pay for test/procedure and (2) make known to (name of your facility) their desire to have information regarding the procedure/test held in confidence and not released to third parties. Any employee who receives such a request must immediately inform (name of responsible party in your facility) who will flag the information as being restricted.[1] HIPAA allows for the release of restricted PHI (1) in compliance to a subpoena; (2) in compliance to statutory reporting requirement; or (3) upon receiving an unrestricted, HIPAA compliant authorization for release of medical records from the patient, patient's legal representative, or executor of deceased patient's estate.

VIII. Policy regarding charges for e-copies of medical records

The Privacy Rule permits the Covered Entity (a healthcare provider) to impose reasonable, cost-based fees for paper copies (See Addendum I, page 6).

According to HITECH the covered entity may charge for the labor cost of making the e-copy. This does not include the cost for searching the data base to find appropriate medical record(s). Currently (October 1, 2010) there is no guidance regarding whether the covered entity is allowed to charge for the cost of the media on which the e-copy is provided to the patient—i.e. CD, flash drive, etc.

[1] This contemplates development and implementation of appropriate software programming with your electronic medical records (EMR) vendor.

IX. Business continuity

[Refer to Medical Interactive's *Hurricane Disaster Preparedness* CD for forms needed to prepare facility specific Disaster Recovery/Business Continuity Plan. After your facility's plan is developed, insert it here]

X. HIPAA Incident/Breach Investigation

Any incident in which the privacy/security of a patient's PHI may have been compromised will be immediately reported to (replace with name of appropriate individual). An incident investigation will be initiated without unreasonable delay. The HIPAA Officer will establish an Incident Response Team (IRT) to investigate incidents and determine if the incident rises to the level of a breach. Refer to definition of IRT on page 8. The procedure for conducting HIPAA incident/breach investigation is located in Addendum II, page 7.

XI. Sanction Policy

All employees will receive training regarding (Your organization's name)'s policy for sanctioning employees who violate our HIPAA privacy/security policy. Employees shall receive training prior to assuming work duties and annually thereafter.[2] (Your organization's name)'s HIPAA sanction policy is located in Addendum III, page 17.

XII. Document Retention Policy

a. All HIPAA documentation such as policy and procedures, risk assessment, incident investigation, breach notification, and training records will be maintained for at least six years[3] in the HIPAA records and documentation section of this policy beginning on page [create a section in your HIPAA policy/procedure manual/file labeled Misc. Documents].

[2] Note: HIPAA requires "periodic" training but does not specify the time frame—annually is recommended by most HIPAA Officers.

[3] Standard (Documentation) (Time Limit) Sec. 164.316(b)(2)(i)