Sample Administrative Requirements for the Implementation of HIPAA

D R A F T [Date]

Administrative Requirements for the Implementation of HIPAA

Purpose:

To issue instructions regarding the Department's obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA), **[add cite]**, and regulations promulgated thereunder, 45 CFR Parts 160, 162 and 164.

Applicability:

This policy applies to all [Practice name] employees.

Definitions:

Protected Health Information (PHI) means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Workforce Members means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the department, its offices, programs, or facilities, is under the direct control of the department, office, program, or facility, regardless of whether they are paid by the entity.

Business Associate (BA) means a person or entity who, on behalf of the department, or an office, program or facility of the department, but not in the capacity of a workforce member, performs, or assists in the performance of, a function or activity involving the use or disclosure of PHI, or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services involving disclosure of PHI.

Privacy Notice means the notice of privacy practices relating to an entity's use and disclosure of PHI that is mandated under HIPAA regulations for distribution to all individuals whose information will be collected by or on behalf of the entity. *See Policy # _____.*

Policy:

A. Personnel Designations: The practice must designate and document designations of the following:

- **Privacy Officer:** The practice must designate an individual to be the Privacy Officer, responsible for the development and implementation of department wide policies and procedures relating to the safeguarding of PHI.

- **Contact Person or Office:** [Practice name] shall designate an individual, position title, or office that will be responsible for receiving complaints relating to PHI and for providing information about the facility's privacy practices.

B. Training Requirements: The practice must document the following training actions:

- On or before the effective date of the HIPAA privacy regulations [4/14/03], all [Practice name] employees and other workforce members must receive training on applicable policies and procedures relating to PHI as necessary and appropriate for such persons to carry out their functions within the department.

- Each new workforce member shall receive the training as described above within a reasonable time after joining the workforce.

- Each workforce member whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a change in position or job description, must receive the training as described above within a reasonable time after the change becomes effective.

C. Safeguards: Each office, program, or facility of the practice must have in place appropriate administrative, technical, and physical safeguards to reasonably safeguard PHI from intentional or unintentional unauthorized use or disclosure.

D. Complaint Process: Each office, program, or facility of the practice must have in place a process for individuals to make complaints about the entity's HIPAA policies and procedures and/or the entity's compliance with those policies and procedures, and must document all complaints received and the disposition of each complaint.

E. Sanctions: The applicable Human Resources Officer for [Practice name] must have in place, must apply, and must document application of appropriate sanctions against workforce members who fail to comply with HIPAA policies and procedures. [Note - there are exceptions for disclosures made by workforce members who qualify as whistleblowers or certain crime victims.]

F. Mitigation Efforts Required: Each staff member must mitigate, to the extent practicable, any harmful effects of unauthorized uses or disclosures of PHI by the entity or any of its business associates.

G. Intimidating or Retaliatory Acts and Waiver of Rights Prohibited:

- **Prohibition on Intimidating or Retaliatory Acts**: No employee of the practice shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against

any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in a HIPAA related investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA regulations as long as the action does not involve disclosure of PHI in violation of the regulations.

- **Prohibition on Waiver of Rights:** No employee of the practice shall require individuals to waive any of their rights under HIPAA as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

H. Policies and Procedures: The practice must document the following actions relating to its policies and procedures:

- **Required Policies and Procedures:** The practice shall design and implement policies and procedures to assure appropriate safeguarding of PHI in its operations.

- **Changes to Policies and Procedures:** The practice must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. The entity also may make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, the entity must may correlative changes in its Privacy Notice. The entity may not implement a change in policy or procedure prior to the effective date of the revised Privacy Notice. [Note - in our policy relating to Privacy Notices, we are requiring that any such notice specifically state that the right to amend is retained.]

I. **Documentation Requirements:** The practice must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the HIPAA regulations, for a period of six (6) years from the later of the date of creation or the last effective date.