WOODLAND CENTERS, INC. Policy Manual	APPROVED: CONCURRED:	POLICY NO. WCI-A-204 EFFECTIVE DATE: 09/2003 REVISION DATE 03/2008 Page: 1 of 3

I. SUBJECT: Risk Management Plan

II. APPLICABILITY: All full-time and contract employees, independent contractors, students, and the Board of Trustees are responsible for compliance with this policy and the agency's risk management plan.

III. PURPOSE: To establish a plan to identify assets that need protection, determine what risks exist, evaluate the likelihood of those risks and the extent of harm they might cause; and developing measures to reduce, eliminate, or guard against those risks in all areas including but not limited to finance, information systems, human resources, clinical/med-somatic, insurance, buildings, vehicles, and equipment.

IV. POLICY: It is the policy of Woodland Centers, Inc. to identify, analyze, develop safeguards for, and monitor potential risks to its operations, employees, and clients in compliance with HIPAA and all other applicable laws, regulations, and standards. The chairperson of the Risk Management committee will be designated by the Executive Director and tied to the Corporate Compliance Committee, Safety Committee, Quality Improvement Committee, and the agency's performance improvement activities.

V. PROCEDURE

A. The Risk Management group will meet at least quarterly to conduct a risk assessment, review exposures, develop action plans to control exposures, and conduct ongoing monitoring of those actions. Minutes of these meetings will be maintained by the chairperson or designee. Members of this group will include:
   1. Executive Director (representative from Corporate Compliance Committee),
   2. Clinical staff as assigned (representative from QI Committee),
   3. Compliance Director/Privacy Officer,
   4. Fiscal Officer (chairperson),
   5. Manager of Human Resources,
   6. Environmental Services Supervisor (representative from Safety Committee), and
   7. MIS Specialist.
   8. Other staff may be included as appropriate.

B. Risk Analysis – The agency will conduct periodic risk assessments to identify and prioritize potential risks, develop action plans to reduce or eliminate those risks, and monitor and evaluate the implementation of

those plans. At minimum, the following areas of potential loss exposure will be considered:

1. Loss of financial cash flow
2. Permanent loss or corruption of electronic PHI
3. Temporary loss or unavailability of medical records
4. Unauthorized access to or disclosure of PHI
5. Loss of physical assets (buildings, computers, equipment)
6. Damage to reputation and public confidence
7. Threats to client safety
8. Threats to employee safety
9. Insurance claims (vehicles, malpractice, Workers' Compensation, fleet insurance, bonding, etc.
10. Litigation (grievances, sexual harassment, EEO, etc.)
11. Incident reports (reportable and non-reportable client related incidents, Safety and Health incidents, and PHI incidents)

C. Risk Controls – Once risks have been identified and prioritized, the agency will determine what mechanisms are already in place to reduce or eliminate these risks, and what actions may need to be taken in those areas which have not already been addressed.

1. While cost is clearly a factor in determining what security measures to implement, the agency will make every effort to ensure that there are adequate budget considerations for managing high priority risks.
2. Staff will be made aware of risk controls as applicable to their positions. This may be communicated in all-staff meetings, one-on-one supervision, or via other methods as appropriate.

D. Risk Monitoring and Evaluation – Actions taken to reduce or eliminate risk will be monitored on a regular basis as part of the agency's performance improvement activities.

1. The risk assessment will be updated at least annually.
2. A report to the Board of Trustees will be prepared at least annually that includes, at minimum, a list of prioritized risks, a summary of actions taken to mitigate those risks, a list of actual losses/exposures that occurred during that past year, and what actions were taken as a result.
3. The Risk Management Committee will review the annual reports from Safety and QI to ensure coordination of and accountability for identified corrective actions.

4. Documentation related to Risk Management will be maintained for a minimum of six (6) years.

E. Violations

1. Staff who willingly or knowingly commit such actions that result in an exposure, loss, and/or liability for the agency shall be subject to disciplinary action up to and including discharge.
2. Such actions may include, but are not limited to:
    a. Hacking into the computer system.
    b. Falsifying information on incident reports, insurance claims, Service Activity Logs, and other agency-related documents.
    c. Not informing Human Resources of driver's license violations.
    d. Deliberate acts of vandalism, sabotage or terrorism.
    e. Improper use or disclosure of PHI.
    f. Abuse or neglect of a client by a staff person.
    g. Improper/unauthorized use of agency funds.
3. Violations of this policy will be brought to the Risk Management Committee for review and investigation and referred to the Corporate Compliance Committee as appropriate. Any disciplinary action as a result of such violation will be determined by the Executive Director based on the results of the Committee's investigation and recommendations.

Questions regarding this policy should be directed to the Risk Management Committee Chair, Compliance Director, or Executive Director.