Creation Date: 05/02/2013
Revision Date: 05/02/2013
Board Approval Date: 12/18/2013
Revision: A

Internal Audit Policy

1. **Introduction**
    a. Clark County has adopted this Internal Audit Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulations, and the Joint Commissions on Accreditation of Healthcare Organizations ("JCAHO") accreditation standards, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements.
    b. This policy controls use of Clark County's health data, media, and computer assets wherever located. All personnel of Clark County must comply with this policy. Familiarity with the personnel security policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

2. Policy
    a. Clark County will institute internal audit of health and other critical information in its system to ensure the integrity of such data and will audit data users' activities to ensure compliance with laws, regulations, professional ethics, accreditation requirements, and its own policies and procedures.
    b. With Regard to Data Quality:
        i. Overall control of data quality is the responsibility of the IT department. At a minimum, he or she will maintain an access log of who accessed which computer objects, when, and for what amount of time, including, but not limited to, logins and logouts, accesses or attempted accesses to files or directories, execution of programs, and uses of peripheral devices.
        ii. He or she will conduct performance audits as needed to measure whether the system meets the medical and/or business objectives for which it was designed and to measure whether the system meets its design objectives in terms of performance.
        iii. Department heads are responsible for advising the IT department of required data integrity standards for data that they maintain, use, and transmit and any problems with data integrity.
    c. With Regard to Data Users' Compliance with Laws, Regulations, Professional Ethics, and Accreditation Requirements:
        i. Responsibility for auditing data users' access to and use of Clark County's information assets rests with the IT department.
        ii. The IT department, in conjunction with the appropriate department head, will take the following steps:
            1. Install intrusion detection software to detect unauthorized access.
            2. Develop audit criteria specifying what activities are to be audited.

3. Perform audits of records of system activity, such as logon, logoff, file access, attempted logon, failed logon, and so forth, and maintain the audit trails for not less than six years from the date of the audit.
4. Perform vulnerability tests to highlight weaknesses in the system.
5. Maintain a log of security-relevant events that have occurred, listing each event and the person responsible.
6. Report security breaches detected during audit pursuant to the Clark County's Report Procedure.
7. Investigate security breaches detected during audit pursuant to the Clark County's Response Procedure.
8. Take appropriate remedial action to mitigate the harm of breaches and prevent recurrence.