Creation Date: 05/02/2013
Revision Date: 08/27/2013
Board Approval Date: 02/17/2013
Revision: A

# Media Controls Policy

## 1. Introduction

a. Clark County has adopted this Media Controls 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. 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. Data, media, computers, and other information assets may not be removed from Clark County without the written consent of the appropriate department head. Such consent may consist of a blanket authorization for certain personnel, such as employed medical professionals, to remove and use such assets offsite.

b. If an employee, agent, independent contractor, or other authorized individual wishes to use personal information assets, such as a personal computer, palm pilot, or similar device, and the like, he or she must obtain the permission of the appropriate department head. The request for and granting of such authorization manifests the individual's consent to be governed by this and all other relevant information security policies, such as the personal computer policy.

c. Conditions for offsite use of data, media, computer, or other information assets include the following:

    1) Data, media, supplies, or information assets of Clark County are not to be used for private purposes or for unauthorized reasons, such as unapproved research.

    2) When such assets are off the premises of Clark County, they must be under the care and control of the person authorized to remove and use the assets.

    3) Other than for blanket authorizations , data users must fill out and submit an off-premises use form and have it approved by their department director. In cases in which any loss or damage to information assets is the fault of the user, the user must be responsible for replacement and/or repair costs that Clark County's or homeowner's insurance deductibles. If the loss or damage is the fault of the user and the loss or damage is not covered by insurance, the data user is responsible for all replacement and/or repair costs. Clark County may deduct such costs from the user's paycheck(s).

d. Users must immediately report all losses of or damage to such equipment to their department director and the security officer. Breaches of confidentiality and other reportable incidents must be reported in accordance with Clark County's Report Procedure.
e. Users will use appropriate safeguards for all assets, such as locking cables for portable computers, as required by their department director and/or the security officer. Assets, such as computers, palm pilots, or floppy disks, must not be left lying around unattended. Users must secure media in appropriate locations, such as a locked cabinet.
f. Clark County's Portable Computer Policy supplements this policy for such assets.