Creation Date: 05/02/2013
Revision Date: 10/29/2013
Approval Date: 12/18/2013
Revision: A

External Drive Security Policy

1. **Introduction**
    a. Clark County has adopted this USB and Flash Drive Security Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Department of Health and Human Services ("DHHS") security and privacy regulations' requirement to protect the security of electronic health information, as well as to fulfill our duty to protect the confidentiality, integrity, and availability of confidential medical information as required by law, professional ethics, and accreditation requirements.
    b. All personnel of Clark County must be familiar with the policy, and demonstrated competence in the requirements of the policy is an important part of every Clark County employee's responsibilities.

2. **Policy**
    a. Clark County encourages the business use of flash drives to increase productivity. Because using personal flash drives is prohibited, see below, the flash drives and the data that they contain are part of the business equipment and data of Clark County, are owned by Clark County, and are not the property of the users of the system. Consequently, flash memory users *do not have a right to privacy in their use of the computer system or its USB flash drive component.* Clark County reserves the right to monitor, audit, delete, and read data on flash drives. The network administrator may override user passwords. The facility may monitor the contents and usage of flash drives to support operational, maintenance, auditing, security, and investigative activities. Users should use flash memory devices with the knowledge that Clark County may from time to time examine the content of such devices. Although this policy prohibits the use of flash memory for personal matters, Clark County cannot guarantee that, if the flash drive is used for such improper purposes, the data will be private. Use of Clark County's flash drives constitutes consent to this policy even if the data user has not signed the required flash drive compliance statement.
    b. No member of the Clark County workforce will use any flash memory or similar device that is not provided by the facility. In other words, no personal flash memory or other devices will be used by any member of the workforce.
    c. Workforce members desiring to use flash memory devices must obtain permission from the HIPAA Security Officer, must complete required training, and must sign the required flash drive compliance statement.
    d. The HIPAA Security Officer is responsible for issuing flash memory devices in such a manner that such officer can track those devices inside and outside the network. The Security Officer must maintain a database for such devices to track them.
    e. The HIPAA Security Officer will implement security measures, such as encryption or password protection. Users must never share passwords or reveal them to anyone else.

f. The HIPAA Security Officer will, after performing risk analysis, determine whether and for how long after no activity desktops should be locked down and ensure this security measure is reflected in the Clark County's policy on workstation use.
g. The HIPAA Security Officer is responsible for performing a risk analysis of malware risks and implementing security measures to protect against such risks.
h. The HIPAA Security Officer is responsible for performing risk analysis to determine whether and which USB ports should be disenabled and how to technically limit access to authorized devices.
i. The HIPAA Security Officer will conduct periodic audits for compliance with this policy and report the results of such audits to the HIPAA Privacy Officer.
j. Workforce members using flash memory devices are responsible for physical security of such devices, such as by having them on a chain that links them to the member's body or otherwise maintaining physical custody of the device.
k. Generally, flash memory users must restrict their use of the email system to proper business purposes relating to the care and treatment of patients and related administrative matters, such as billing. Although the email policy allows limited personal emails, such as telling a spouse that one has to work late, *no personal data whatsoever may be stored on a Clark County flash drive.*
l. The HIPAA Security Officer is responsible for providing required training and for, in conjunction with the HIPAA Privacy Officer, keeping documentation of the training and the signed flash drive compliance statement for at least six (6) years.
m. All workforce members must immediately report any breaches of security, confidentiality, or this policy to the HIPAA Security Officer [add any other official, such as the immediate supervisor, HIPAA Privacy Officer, compliance officer, or any other member of management that is appropriate for your situation] and take appropriate action to prevent further harm or otherwise mitigate the breach.