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

Portable Computer Policy

1. Introduction

a. Clark County has adopted this Portable Computer Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and with the Department of Health and Human Services ("DHHS") security and privacy regulations' requirement to protect the security of electronic health information, with the Joint Commission 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 who use laptop, notebook, or other portable computers must be familiar with the policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every Clark County employee's responsibilities.

2. Policy

a. Officers, agents, employees, contractors, and others using portable computers (users) must read, understand, and comply with this policy.

b. No person may use a personal computer for Clark County's business purposes without the authorization of the department hear or the IT department. No user may, for any purpose, download, maintain, or transmit confidential patient or other information on a personal computer without the written authorization of department hear or the IT department .upon the recommendation of the user's supervisor.

c. Clark County has issued computer equipment to you for the uses for which you have been specifically trained. The hardware, software, all related components, and data are the property of Clark County and must be safeguarded and be returned upon request and upon termination of your employment.

d. Any equipment exchanged must be logged in the server room equipment log. Your responsibility for the initial equipment extends to the issued equipment and/or any exchanged or additional equipment that Clark County may issue to you during your employment.

e. User agrees to use the equipment solely for Clark County's business purposes.

f. User further understands the following:

1) Dial in functions are restricted to dialing into Clark County.

2) User is not permitted to dial into any other unauthorized services, internet service providers, or any other internet access or to use the dial-up capabilities in any other manner than as instructed. The user understands that the hardware has been disabled from performing any functions other than those intended for business use and that the user may not attempt to

enable such other functions. Computers, associated equipment, and software are for business use only, not for the personal use of the user or any other person or entity.

3) User will not download any software onto the computer except as loaded by authorized staff of the IT department.
4) User will not insert floppy disks, CDs, DVDs, or any other media into the computer without the authorization of the department head.
5) User must use only batteries and power cables provided by Clark County and may not, for example, use car adaptor power sources.
6) User will not connect any additional peripherals (keyboards, printers, modems, and so forth) without the authorization of the IT department.
7) User is responsible for securing the unit, all associated equipment, and all data within homes, cars, and other locations as instructed in the training provided.
8) Users will use the cable provided to lock equipment to immovable objects except when transporting the equipment.
9) User may not leave mobile computer units unattended unless they are in a secured location.
10) User should not leave mobile computer units in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.
11) User must place portable computers and associated equipment in their proper carrying cases when transporting them. The case must display the user's name and identify the covered entity.
12) User must not alter the serial numbers and asset numbers of the equipment in any way.
13) User will not permit anyone else to use the computer for any purpose, including, but not limited to, the user's family and/or associates, patients, patient families, or unauthorized officers, employees, and agents of Clark County.
14) User must not share passwords with any other person and must safeguard passwords and may not write them down so that an unauthorized person can obtain them.
15) User must report any breach of password security immediately to the IT department.
16) User must maintain patient confidentiality when using the computers, as specified in Clark County's Workstation Policy. The user must protect the screen from viewing by unauthorized personnel, and the user must properly log out and turn off the computer when not using it.

17) User must immediately report any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the IT department.