Creation Date: 05/02/2013
Revision Date: 10/29/2013
Approval Date: 12/182013
Revision: A

Workstation Use Policy

1. **Introduction**
    a. Clark County has adopted this Policy on Workstation Use to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulation's requirement for such a policy, 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 and all covered entity personnel that use computer terminals must be familiar with the contents of this policy and follow its guidance, as appropriate, when using computer equipment. Familiarity with the plan and demonstrated competence in the requirements of the plan are an important part of every Clark County employee's responsibilities.

2. Preventative Measures
    a. All computer users will monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. For example, if air conditioning fails, so that the temperature around the computer may exceed a safe level, the user must immediately notify IT department and maintenance.
    b. All computers plugged into an electrical power outlet will use a surge suppresser approved by the IT department.
    c. All personnel using computers will familiarize themselves with and comply with the covered entity's disaster plans and take appropriate measures to protect computers and data from disasters.
    d. Personnel using computers will not smoke at or near the terminal nor eat or drink at the terminal to prevent damage due to spills and so forth.
    e. Personnel logging onto the system will ensure that no one observes them entering their password.
    f. After three failed attempts to log on, the system will refuse to permit access and generate a notice to the system administrator.
    g. Personnel will not log onto the system using another's password nor permit another to log on with their password. Nor will personnel enter data under another person's password.
    h. Each person using the covered entity's computers is responsible for the content of any that data he or she inputs into the computer or transmits through or outside the covered entity's system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All personnel will familiarize themselves with and comply with the covered entity's email policy.

i. No employee may access any confidential patient or other information that they do not have a need to know. No employee may disclose confidential patient or other information unless properly authorized.
j. Employees must not leave printers unattended when they are printing confidential patient or other information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.
k. Employees may not use the covered entity's system to solicit for outside business ventures, organizational campaigns, political activities, or religious causes. Nor may they enter, transmit, or maintain communications of a discriminatory or harassing nature or materials that are obscene or x-rated. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain, or transmit any abusive, profane or offensive language.
l. Personnel using the computer system will not write down their password and put it at or near the terminal, such as by putting the password on a yellow "stickie" on the screen or a piece of tape under the keyboard.
m. Each computer will be programmed to generate a screen saver when the computer receives no input for a specified period. Supervisors may specify an appropriate period to protect confidentiality while keeping the computer available for use.
n. Personnel must log off the system if they leave the computer terminal for any period of time.
o. Each department head may develop a policy on hard-copy printouts, including who may generate such printouts, what may be done with the printouts, how to dispose of the printouts, and how to maintain confidentiality of hard-copy printouts.
p. No personnel may upload any unauthorized software or data. The IT department must approve any software or data that an employee wishes to upload. This rule is necessary to protect against computer viruses from being transmitted into the covered entity's system.