Personnel Security Policy

1. Introduction

a. Clark County has adopted this Personnel Security 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. Along with its other policies and procedures protecting the integrity and confidentiality of health information, Clark County adopts this personnel security policy to ensure that its employees and others who have access to health information are properly screened, properly trained, and properly supervised regarding their access to and use of health information.

3. Screening of Individuals with Access to Individually Identifiable Health Information

a. HIPAA and the DHHS security regulations require "appropriate clearances" for all personnel with access to individually identifiable health information. The regulations do not, however, specify what appropriate clearances consist of. Rather, they leave it up to covered entities to determine what screening is appropriate based on a risk analysis, defined as the process of selecting cost-effective security/control measures by balancing the cost of those measures against the harm that would occur if those measures were not in place.

b. Thus, each department head is responsible for screening all employees and others with access to individually identifiable health information. An appropriate clearance may include, among others, the following elements:

1) Criminal background check.
2) Credit check.
3) Verification of references.
4) Verification of employment history.
5) Verification of licensure and/or certification.
6) In-depth interview.
7) Drug testing.
8) Clauses in vendor contracts, such as for computer system maintenance technicians, that require the vendor to screen employees with access to our system and data.

9) Agreements with other entities requiring them to screen personnel with access to our system and data.
10) Self-certification in the employment application.

c. Department heads will determine what screening is appropriate for its personnel with access to confidential health information by considering the risk and then balancing the cost of the security measure against the risk. Factors to consider when evaluating the risk include the following:
    1) Background of the class of employee (average age, educational experience, specialized training, licensure or certification, and the like).
    2) Level of access of the class of employee or of the particular employee. An individual who has access to the entire system or to a file server poses a greater risk than one who can log in at only one workstation and who does not have access to all data.
    3) Nature of the data user's duties. Access to particularly sensitive medical data, such as information regarding AIDS/HIV, mental health, alcohol and drug abuse, sexually transmitted diseases, and the like, or to financial information, may pose greater risks than access to more routine matters, such as scheduling.
    4) History of data users in that department.
d. Department heads may "grandfather" or not conduct a further screening of employees and others with access if the data user has had no breaches of confidentiality in the last three years.
e. The physician credentialing process constitutes sufficient screening for access to patient information.
f. Directors will retain records of screening for not less than six years from the completion of the screening.

4. Training

a. HIPAA and the DHHS security and privacy regulations require training all personnel with access to individually identifiable health information. Training is an integral part of personnel security. All department heads are responsible for training personnel with access to health information as required by Clark County's training policy.

5. Supervision

a. Properly screening and training personnel with access to individually identifiable health information is not enough. Employees and others with access must be continually reminded of their responsibilities concerning protection of health information. Therefore, supervisors must take the following steps:
    1) Detail security and confidentiality requirements in position descriptions and performance evaluations. Adherence to security and confidentiality policies must be part of every data user's performance evaluation process.

2) Monitor the day-to-day performance of data users to detect problems with security and confidentiality before they become serious breaches.
3) Audit compliance with security and confidentiality policies in accordance with the Clark County's Information Audit Policy.
4) Report breaches of security or confidentiality in accordance with the Clark County's Report Procedure.
5) Respond to breaches of security or confidentiality in accordance with the Clark County's Response Procedure.
6) Commend data users demonstrating a high degree of proficiency in protecting data integrity and confidentiality.
7) Take appropriate sanctions against data users who breach security/confidentiality in accordance with Clark County's sanction policy.