Creation Date: 10/29/2013
Revision Date: 10/29/2013
Approval Date: 12/19/2013
Revision: A

Access Establishment Policy

1. Introduction

a. Clark County has adopted this Access Establishment Policy to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department Health and Human Services ("DHHS") security and privacy regulations, 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. This policy governs what steps occur after employee is authorized to access individually identifiable health information and to the system components that contain such data. All personnel of Clark County must comply with this policy. Familiarity with this policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

2. Policy

a. Access establishment is the process of granting access to an authorized data user, one who has been authorized access under Clark County's Access Authorization Policy.

b. Upon receipt of a request to provide access to a named individual, the Personnel department will determine whether any reason exists to deny the request. Grounds for denial include, but are not limited to, the following:
   i. Noncompliance with requirements of the Access Authorization Policy.
   ii. Security risk unknown to the requester.
   iii. Refusal of prospective data user to sign required documents.
   iv. Inability of prospective data user to properly use applications and system assets after training.

c. The Personnel department will work with the requester to resolve cases in which the former initially denies access. If the matter cannot be resolved, the Personnel department will report the matter to the Privacy Officer for resolution.

d. Upon granting access, the IT department shall take the following steps:
   i. Assign the data user unique user identification.
   ii. Assign the data user an initial password.

e. The IT department shall take the following steps regarding Clark County employee access:
   i. Establish password guidelines
      1. Passwords are to be random and comply with the following requirements:
         a. Must be at least eight characters in length.

b. Does not consist of the data user's name, spouse's name, parents' names, children's' names, or any easily determinable password combinations.

ii. Maintain a list of unique user identifications and related passwords in a location other than on a Clark County system or computer asset.

iii. Require data users to sign a statement regarding use of passwords that prohibits them from—

1. Writing down the password.
2. Disclosing the password to another person or entity other than to the IT department and/or his or her designee.
3. Recording the password in Clark County's system or any other system.
4. Transmitting the password online, particularly by email.
5. Any other practice that the IT department believes would put the availability, accuracy, or confidentiality of Clark County's data, media, or equipment at risk.

iv. Communicate to data users that failure to observe the rules governing passwords may result in disciplinary action up to and including termination in accordance with Clark County's sanction policy.

f. The IT department may:

i. Modify access in accordance with Clark County's Access Modification Policy;

ii. Suspend access when appropriate to respond to a breach of confidentiality/security in coordination with Clark County's Report and Response Procedures; or

iii. Terminate access when notified to do so in accordance with Clark County's Termination Procedure.