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

Access Modification Policy

1. Introduction

a. Clark County has adopted this Access Modification 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 how access can be modified to 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 modification is the process of changing the access to Clark County's data and systems by an authorized data user, one who has been authorized access under Clark County's Access Authorization Policy and has had access established under Clark County's Access Establishment Policy.

b. Bearing in mind that, under Clark County's policies, no person should have access that does not need access, and no person should have more access than necessary.

c. Clark County may determine that an individual or a group of individuals need more, less, or otherwise changed access because of a change in duties or a change in status, such as full-time to part-time, employee to outside contractor, completion of a project, and the like.

d. When a supervisor makes such a determination, he or she should request that the IT department or his or her designee change the current level of access to another level of access.

e. Upon receipt of a request to change a named individual's or individuals' access, the IT 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.

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

g. Upon granting the changed level of access, the IT department will take the following steps:
    i. Take necessary measures to change the level of access.

ii. Assign a new unique identifier, if necessary.
iii. Assign the data user a new initial password, if necessary.
iv. Make necessary changes to the list of unique user identifications and related passwords.
v. Require data users to sign a new statement regarding use of new passwords.
vi. Train personnel with changed access, as necessary, in aspects of system use appropriate to their changed access.
vii. Maintain records of the changed access, new security statements, and/or completed training.