Creation Date: 05/02/2013
Revision Date: 10/29/2013
Approval Date: 12/18/2013
Revision: A

Termination Procedure Policy

1. Introduction

a. Clark County has adopted this Termination Procedure 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, 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 must comply with this policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

2. Policy

a. HIPAA and the DHHS security and privacy regulations require termination procedures for all personnel with access to individually identifiable health information.
b. The department head or the Personnel department are responsible for notifying the IT department of employees and others, such as independent contractors, who will be leaving Clark County's employ or otherwise (through reassignment, extended absence, and so forth) and will no longer need access to health information.
c. The department head or the Personnel department are responsible for notifying the IT department of employees and others, such as independent contractors, who through reassignment or otherwise no longer need the level of access that they had had so that their level of access can be adjusted.
d. Any other data user who becomes aware that a data user is leaving the covered entity either permanently or for an extended or unexplained absence should report the matter to the IT department for a determination of whether to revoke/suspend that person's access.
e. Employees and others who are terminated may expect to have their data access immediately terminated and not to receive any final pay due until the termination of access procedure is properly completed.
f. Upon termination of an employee or other person with access, the IT department will take the following actions:
    i. Revoke access privileges, such as user IDs and passwords, to system and data resources and secure areas.
    ii. Retrieve sensitive materials, including access control items, such as keys and badges.
    iii. Retrieve all hardware, software, data, and documentation issued to or otherwise in the possession of the data user.
    iv. Arrange for an exit briefing to verify retrieval of all items, to discuss any security/confidentiality concerns with the data user, and to remind

the data user of the continuing need to protect data security and patient confidentiality.

v. Notify Personnel department of completion of the termination procedure so that the data user can receive any final pay due.

g. Keep records of the termination procedure for each such person, including the retrieval of security-related items, such as badges, passwords, and information system assets, for not less than six years from the termination date.

h. When necessary, the Personnel department will arrange for security escort of terminated personnel from the covered entity and for an audit of their accounts to detect any security or confidentiality threats or breaches.