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

Health Information Data Backup Plan

1. Introduction

a. Clark County has adopted this Health Information Data Backup Plan to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department Health and Human Services ("DHHS") security and privacy regulations, and 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 this policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

2. Policy

a. This policy supplements the covered entity's overall security policy, which is intended to protect data integrity, confidentiality, and availability.

b. All personnel (employees, staff, contract workers, and so forth) who have access to health information must read, understand, and comply with this policy.

c. IT department is responsible for performing daily backups (at a minimum) on Clark County's network, including shared drives containing application data, patient information, financial data, and crucial system information.

d. Clark County will back up all such data automatically.

e. Only the IT department, the system administrator, and their designees have access to the backup media and may remove backup media in the case of an emergency.

f. The IT department, the system administrator, or their designees may review backup media to validate the accuracy, completeness, and integrity of the backup.

g. The IT department, the system administrator, or their designees will immediately act upon any errors. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.

h. The IT department is responsible for testing the validity of backup media and to restore the data in the event of a computer system problem, failure, or other disaster at least monthly and more often if necessary to ensure data integrity, availability, and confidentiality.

i. Responsible personnel must enter into the network log successful restore functions. Responsible personnel must immediately act on any problems identified during the restore function and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.

j. All personnel who detect or suspect a data backup problem should immediately report the same to the IT department or their respective department head. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    i. Narrative of the data backup problem.
    ii. How long the problem has existed.
    iii. Suggested solutions.