Heritage Provider Network & Affiliated Medical Groups	Program: Management Information Systems			
	Policy No. 14-011	Effective Date: 04/20/2005	Page - 1 -	
	Authored by: Dave Pfafman	Date: 04/15/2005	Revised by: Dave Pfafman	Date: 02/05/2015
	Approved by: Scott Bae	Date: 02/02/2015		
Title of Policy: Data Backup and Retention				

POLICY:

It is the policy of Heritage Provider Network to provide information for management and workforce members for performing periodic computer system backups to ensure that critical data is adequately preserved and protected against loss and destruction.

PURPOSE:

The purpose of this policy is to create a backup and recovery process for Heritage Provider Network's computers, networks and systems must be documented and reviewed annually and tested on a regular basis.

PROCEDURE:

The backup should, at a minimum, include:

1. Physical Access Controls
   a. The minimum acceptable level of physical security for any backup system or server(s) is to place it behind a locked door.
   b. Physical access to backup equipment must be approved by the Security officer.

2. Backup schedule
   a. At a minimum, modified data on computers must be incrementally backed up at the end of each work day and a full system backup must be performed at least once per month. Critical data should be backed up, regardless of where it resides. On a weekly basis at least one full backup must be stored off-site.
   b. A process must be implemented to verify the success of the electronic information backup.

3. Backup schedule logs:
   a. The backup software should capture a list of all files and directories encountered and saved. Logs should contain information about successful backups, unsuccessful backups, backup media that was left in place accidentally and overwritten, when and where the media was sent offsite, the success or failure of restore tests and bad media encountered which may affect your ability to obtain files from a previous backup.

PROCEDURE (continued):

3. Backup schedule logs:
    b. Assign a primary and backup workforce member to rotate the media and note any problems or exceptions. Write an entry for successful backups, the date and which media was utilized. Keep the written log with the computer that performs the backup.
    c. Legible, unique labels shall be placed on all backup media.

4. Length of Data Retention
    a. Full system backup should be copied and or archived and not be stored in the same geographic location as the source systems on a weekly basis.
    b. Archived backups must be periodically tested to ensure that they are recoverable.
    c. At a minimum, backup data should be retained for six month-end backup sets as well as all year-end backup sets. The daily backups should be retained for at least two weeks. Retention of daily backups for up to four weeks is preferred.

5. Off Site Storage Procedures
    a. Archived backups which can restore to the most recent business days shall be stored off site. Heritage Provider Network will contract with a vendor to provide backup storage.
    b. Security access controls implemented at offsite backup and storage facilities must meet or exceed the security access controls of the source systems.

6. Documentation
    a. The backup restore and recovery processes must be documented.
    b. What is backed up, when, and how often the backups occur must be documented.
    c. A list of mission critical servers and type of data contained on each server.
    d. Procedures and processes to restore backup client.
    e. Procedures and processes to restore backup server.
    f. Reconstruction times for the existing data backup system.
    g. Contact information:
        i. List of designated staff to be contacted in an emergency. A copy of this list must be kept in a secure location, such as with off-site backups, and be readily accessible in case of an emergency

PROCEDURE (continued):

6. Documentation

g. Contact information:
   ii. Vendor contact and support information
   iii. Offsite storage contacts
h. License codes and media.
i. Hardware and software for data backup system

7. Backups must be performed in accordance with the backup documentation for that backup system.

Unacceptable Use

1. The following activities are prohibited. Heritage Provider Network workforce members may be exempted from these restrictions during the course of their job responsibilities (e.g., systems administrators and computer technicians may have a need during maintenance periods to disable computer or network access.).

2. Under no circumstances is a workforce member of Heritage Provider Network authorized to engage in any illegal activity while utilizing Heritage Provider Network resources.

Unacceptable use activities include, but are not limited to the following:

1. The backup system is not considered to be an electronic archiving process for the storing of files for future retrieval. The backup system is to be used for the purposes of disaster recovery only.

2. Data retention systems are available for Heritage Provider Network data only. Users may not store personal or non-Heritage Provider Network information on any Heritage Provider Network data retention system.

PROCEDURE (continued):

Enforcement

1. Heritage Provider Network's Security Officer is responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.