Heritage Provider Network & Affiliated Medical Groups	Program: Management Information Systems			
	Policy No. 14-024	Effective Date: 04/20/2005	Page - 1 -	
	Authored by: David Pfafman	Date: 04/14/2005	Revised by: Scott Bae	Date: 02/02/2015
	Approved by: Scott Bae	Date: 02/02/2015		
Title of Policy: Device and Media Controls				

POLICY:

It is the policy of Heritage Provider Network to provide information for management and workforce members in prescribing formal practices that secure electronic patient protected health information and proper destruction of such data.

PURPOSE:

The purpose of this policy is to provide information for management and workforce members for maintaining formal practices for monitoring the receipt, re-use, removal and disposal of all hardware, software, media, and electronic devices containing electronic protected health information.

PROCEDURE:

Receiving Hardware and Software

1. Only personnel authorized by HPN shall receive hardware and software that contains electronic data.

2. All hardware and software received by HPNcontaining individually identifiable protected health information will be documented. The documentation shall include a receipt of delivery and a notation of the acceptable condition of the hardware and software.

3. All hardware and software will be labeled for identification.

4. All application software and hardware systems will be scanned for viruses and other malicious software prior to delivery.

5. A backup will be made of all software received and stored securely.

6. A receipt will be made documenting the delivery of all hardware and software containing individually identifiable protected health information and all components will be identified and labeled and listed in a master inventory of all electronic devises and media containing individually identifiable protected health information.

7. All hardware and software containing individually identifiable protected health information will be physically inventoried on a regular basis and the inventory will be documented.

Removing Hardware and Software

1. Written request must be made and approval must first be obtained from HPN's Security Officer prior to the removal of any hardware or software containing individually identifiable protected health information. It can also be noted based on the individual's job requirements.

2. The Security Officer will assess the reasons for the request, and, will take into consideration the following when making a determination to grant the request:
   a. The requestor's access and clearance levels
   b. The requestor's job requirements
   c. The sensitivity of the components
   d. The period and frequency of removal
   e. Any applicable policies and Business Associate agreements.

3. A signed approval detailing the components and dates of removal will be required before they can be removed.

Disposal of Electronic Data Including Hardware and Software

1. Prior to disposal, all hardware, software, media and electronic devices containing individually identifiable protected health information will have all identification labels removed and will then be securely purged of all individually identifiable protected health information or physically destroyed using disk sanitation software. The Security Officer will verify and document the removal of the labels and the purging or disposal.

2. The Security Officer will ensure the master inventory list is appropriately updated upon the disposal of any components containing individually identifiable protected health information.

Re-using Hardware, Software, Media and Electronic Devises

1. Prior to re-use, all hardware, software, media, and all electronic devices containing individually identifiable protected health information will be securely purged of all individually identifiable protected health information. The Security Officer will verify and document the successful purging prior to re-use.

2. Prior to re-use, all identification labels on all hardware, software, media, and all electronic devices containing individually identifiable protected health information will be removed. The Security Officer will verify and document that all labels have been removed.

3. The Security Officer will ensure the master inventory list is appropriately updated upon the re-allocation of all components previously containing individually identifiable protected health information.

ENFORCEMENT:

1. Heritage Provider Network Compliance Committee, Security officer, office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.