 <p style="text-align: center;">Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems			
	Policy No. 14-021	Effective Date: 04/20/2005	Page - 1 -	
	Authored by: Dave Pfafman	Date: 04/14/2005	Revised by: Scott Bae	Date: 02/02/2015
	Approved by: Scott Bae	Date: 02/02/2015		
Title of Policy: Information System Access				

POLICY:

It is the policy of Heritage Provider Network to identify and determine the appropriate level of access to the workforce members the minimum level of protected health information (PHI) residing on all electronic information systems in order to perform their work and to remove access when the needs change.

PURPOSE:

The purpose of this policy is to determine and provide the minimum level of PHI necessary to perform their work functions and to remove their access when the requirements change.


DEFINITIONS:

1. Protected Health Information – Individually identifiable health information that is transmitted or maintained by electronic media or transmitted or maintained in any other form or medium.
2. Individually Identifiable Health Information – Health information which includes demographic information that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual and that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

PROCEDURE:

1. Heritage Provider Network provides access to the Information systems based on the job requirements. The initial request is generated upon new hire by a coordinated communication between the employee’s supervisor and the human resources department. Upon the department manager’s approval, the user is granted the minimum level of access to the PHI necessary to perform their job.
2. The login information will be based on a unique identification name assigned to a specific domain name. Every domain and user identification name determines the employee’s information and their access to PHI. The user can only gain access using this ID and a strong encryption password after verifying that they are the authorized user to access PHI. This ensures that the individuals seeking access to PHI is verified as the one that is claimed.

PROCEDURE (continued):

 <p>Heritage Provider Network & Affiliated Medical Groups</p>	Program: Management Information Systems		
	Policy No. 14-021	Effective Date: 04/20/2005	Page - 2 -
	Authored by: Dave Pfafman	Date: 04/14/2005	Revised by: Scott Bae
	Approved by: Scott Bae	Date: 02/02/2015	Date: 02/02/2015
Title of Policy: Information System Access			

3. The login name or user ID generated by the domain or systems currently used at Heritage determines the unique identification for the individuals accessing the PHI and the user name and ID numbers can be used for tracking purposes to determine access to PHI.
4. HPN will conduct periodic security assessments that will identify appropriate access levels to the various applications containing PHI and make necessary adjustments based on changes in the job requirements.
5. Upon employee terminations, human resources department provides IT department the employee name and the date that the access to the company systems should be removed. Domain access, VPN access, and all application access are removed.

Enforcement

1. Heritage Provider Network's Security Officer, office managers, human resources, and compliance committee 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.