Heritage Provider Network & Affiliated Medical Groups	Program: Management Information Systems			
	Policy No.	Effective Date: 08/17/2000	Page - 1 -	
	Authored by: David Pfafman	Date: 08/17/2000	Revised by: Scott Bae	Date: 02/02/2015
	Approved by: Scott Bae	Date: 02/02/2015		
Title of Policy: Server Security				

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.

PURPOSE:

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Heritage Provider Network. Effective implementation of this policy will minimize unauthorized access to Heritage Provider Network proprietary information and technology.

All internal servers deployed at Heritage Provider Network must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by HPN MIS. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by HPN MIS.

PROCEDURE:

1. Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    a. Server contact(s) and location, and a backup contact
    b. Hardware and Operating System/Version
    c. Main functions and applications, if applicable

2. Information in the corporate enterprise management system must be kept up-to-date.

3. Configuration changes for production servers must follow the appropriate change management procedures.

General Configuration Guidelines

1. Operating System configuration should be in accordance with approved HPN MIS guidelines.

2. Services and applications that will not be used must be disabled where practical.

PROCEDURE (continued):

3. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

6. Always use standard security principles of least required access to perform a function.

7. Do not use root when a non-privileged account will do.

8. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

9. Servers should be physically located in an access-controlled environment.

10. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    a. All security related logs will be kept online for a minimum of 1 week.
    b. Daily incremental tape backups will be retained for at least 1 month.
    c. Weekly full tape backups of logs will be retained for at least 1 month.
    d. Monthly full backups will be retained for a minimum of 2 years.

2. Security-related events will be reported to HPN MIS, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    a. Port-scan attacks
    b. Evidence of unauthorized access to privileged accounts
    c. Anomalous occurrences that are not related to specific applications on the host.

PROCEDURE (continued):

Compliance

1. Audits will be performed on a regular basis by authorized organizations within Heritage Provider Network.

2. Audits will be managed by the internal audit group or HPN MIS, in accordance with the *Audit Policy*. HPN MIS will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

3. Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.