Heritage Provider Network & Affiliated Medical Groups	Program: Management Information Systems			
	Policy No. 14-008	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: Security of Electronic Data and Disk Encryption				

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.

DEFINITIONS:

1. Protected Health Information (PHI) - Individually identifiable health information that is transmitted or maintained in any form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards.

2. Individually Identifiable Health Information - Any information, including demographic information, collected from an individual that 1) is created or received by a health care provider, health plan, employer, health care clearinghouse; and 2) is related to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which a) identifies the individual, or b) there is reasonable basis to believe that the information can be used to identify the individual.

3. Computer Systems - Computers connected to local and statewide communication networks, database storage or electronic records systems, Internet or email.

4. Local Area Network - Electronic network access allowing access to an individual facility’s electronic data and computers.

5. Network Attached Computer - Any computer with access to a local area network and/or the Heritage Provider Network's network.

6. Workforce - Includes employees, volunteers, contract workers, trainees and other persons who are in Heritage Provider Network's facility on a regular course of business. This shall include client workers employed by Heritage Provider Network or any of its facilities.

7. Patient - Any individual who has received or is receiving services from Heritage Provider Network.

8. Restricted Access - Computer systems with access limited to specific systems, activities, or files.

DEFINITIONS (continued):

9. Security Officer - Individual designated by Heritage Provider Network to oversee all activities related to the development, implementation, maintenance of, and adherence to Heritage Provider Network policies and procedures covering the electronic and physical security of, and access to, protected health information and other Heritage Provider Network data in compliance with HIPAA and other federal and state laws and regulations.

10. Media - Backup tapes, hard drives, floppy diskettes, CDs, zip drives cartridges, optical, and paper hard copies.

PROCEDURE:

1. Users shall be automatically logged off their workstations after a maximum period of 15 minutes of inactivity. For more information regarding securing computer workstations review the Information Systems Access Policy and Automatic Logoff Policy.

2. The MIS departments shall spot check an audit trail of all accesses and changes to patient data on a regular basis and report violations to the Security Officer and appropriate staff as designated.

3. Access to Heritage Provider Network networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the auspices of Heritage Provider Network Security Officer.

4. Heritage Provider Network Security Officer shall maintain backup data in accordance with Heritage Provider Network Data Backup and Retention Policy.

5. Heritage Provider Network Security Officer shall ensure that all media has been thoroughly sanitized of any patient data before the media is recycled or disposed of, pursuant to Heritage Provider Network Policy for Disposal of PHI and Policy for Devise and Media Controls.

6. Access to media containing patient data shall be controlled through:
   a. Access control lists to network media.
   b. Physical access control to Heritage Provider Network's hardware.
   c. Purging Heritage Provider Network's data on any type of media before it is recycled or discarded.
   d. Storage of data on media that is backed up.

PROCEDURE (continued):

7. Virus protection for the Heritage Provider Network networks or computer systems shall be maintained by Heritage Provider Network Security Officer. It is controlled and updated when

appropriate.

8. Equipment that has not been purchased by, and is owned by, Heritage Provider Network shall not be allowed to connect to the Heritage Provider Network's network without the permission and authorization of the Security Officer and others as designated.

9. All company desktops and laptops containing PHI will have the hard disks encrypted using Sophos Enterprise Encryption software. It will encrypt all fixed and removable disks including external hard drives and flash drives. Any data containing PHI must be encrypted before transmission to any external sources.

10. To avoid potentially virus-carrying attachments, Heritage Provider Network's workforce shall not allow certain types of attachments, such as executable files to pass through email.

11. Heritage Provider Network Security Officer shall maintain a support contract with software vendor(s) to ensure uninterrupted support.

12. Heritage Provider Network's workforce shall not load software, from any source, onto their assigned workstation or any other Heritage Provider Network's equipment without authorization from the Security Officer. This includes but is not limited to software from the internet, a CD, or removable media. Software shall be loaded on workstations only by designated employees of Heritage Provider Network Security Officer.

13. All confidential data containing PHI should be transmitted via secure transfer methods such as secure FTP, secure email, wireless network security with WPA-2 or better or with the use of PGP encryption process.

14. Heritage Provider Network workstations shall be situated by Heritage Provider Network Security Officer so as to prevent more than incidental observation of work product or other sensitive data.

15. In order to determine potential risks vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information is mitigated, a risk analysis will be performed periodically, no less than annually, using the risk assessment methodology determined by NIST.

PROCEDURE (continued):

The Risk Assessment Methodology consists of the following:

a. System Characterization which consists of hardware, software, system interfaces, data and information, people and system mission to determine the system boundaries and functions, system and data criticality and sensitivity.

b. Threat Identification which consists of history of system attack, data from agencies such as OIG, mass media, etc. to determine the threat statement.

c. Vulnerability Identification which consists of reports from prior risk assessments, any audit comments, security requirements, and security test results to determine the list of potential vulnerabilities.

d. Control Analysis which consists of current controls as well as planned controls to list the current and planned controls.

e. Likelihood Determination which consists of threat-source motivation, threat capability, nature of vulnerability, and current controls to determine the likelihood rating.

f. Impact Analysis which consists of loss of integrity, loss of availability, and loss of confidentiality to determine the impact rating.

g. Risk Determination which consists of likelihood of threat exploitation, magnitude of impact, and adequacy of planner or current controls to determine the risks and associated risk levels.

h. Control Recommendation will consist of recommending the controls that need to be added or modified.

i. Results Documentation will consist of producing the risk assessment report to make the necessary changes to mitigate risks.

16. In addition to all the security measures currently in place, such as security controls, encryption of data and email, etc., based on the Risk Assessment that is performed, all recommended changes are implemented immediately to ensure we are managing and reducing our risks and vulnerabilities to a reasonable and appropriate level.

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.