Heritage Provider Network & Affiliated Medical Groups	Program: HIPAA Compliance			
	Policy No.	Effective Date: 01/01/2012	Page - 1 -	
	Authored by: Compliance Sub Committee	Date: 01/01/2012	Revised by: Sandy Finley	Date: 10/05/2015
	Approved by: Compliance Committee	Date: 10/06/2015		
Title of Policy: Actions to Mitigate Breach Risk				

PURPOSE:

To ensure that corrective action is applied to mitigate the risks and/or damages which result from a breach in a member's personal health information (PHI) or any violation of the Heritage Provider Network and its affiliated Medical Groups (HPN) Compliance Program.

POLICY:

Heritage Provider Network and its Affiliated Medical Groups (HPN) are ethically and legally committed to prevent any violations of non-compliance and immediately correcting any violations by issuing corrective actions and/or implementing system changes to ensure that a similar violation does not occur in the future.

RESPONSIBILITY:

All employees of Heritage Provider Network and Affiliated Medical Groups.

PROCEDURES:

1. Privacy breaches and/or violations of non-compliance are evaluated according to HPN's Compliance Program and Human Resources policies pertaining to appropriate disciplinary actions, which may include: additional training, education, counseling and/or termination.

2. Employees are provided with compliance training (Code of Conduct, Fraud, Waste, and Abuse, HIPAA/HITECH, Model of Care, Injury and Illness, Harassment) in accordance with local, state and federal laws, and are required to follow those guidelines.

3. Employees are required report breaches of patient privacy issues and other violations of non-compliance to their Compliance/Privacy Officer, Supervisor, Human Resources, or to the Compliance Hotline (855-682-4127).

4. The Compliance Officer or designee will promptly address violations and document on the Incident Log. The Compliance Officer will immediately initiate the investigation and will use the monitoring tools associated with identifying any potential non-compliance (e.g. Risk Assessment, Fraud, Waste, and Abuse letter).

5. Compliance tools for identifying employee violations include, but are not limited to: surveillance cameras, internet usage reports, witnesses, phone records, Risk Assessments, FWA letters, and PCG Software.

6. Sanctions against employees or FDRs will be conducted promptly, as appropriate and in accordance with the company's discipline guidelines within 10 days of discovery of non-compliance.

7. Business Associates - Contract Administrator is responsible for obtaining a signed privacy addendum for each and every current and future business associate providing the covered entity with a function or activity involving the use or disclosure of PHI.

    a. Any knowledge of a pattern of activity or practice on the part of the BA that violates or breaches patient privacy or other issue of non-compliance will be addressed immediately.
    b. The BA will be required to take reasonable steps to resolve the breach or non-compliance.
    c. If steps of resolution are unsuccessful, HPN will terminate the BA agreement for non-compliance.
    d. When termination is not possible the problem will be reported to the Secretary of DHHS or other regulatory authorities as required.

8. See also, Routine Monitoring, Auditing, and Investigation of Risks policy and Whistleblower Protection policy for additional procedures for mitigating risk.