DEPARTMENT: Compliance **POLICY TITLE:** CMP08 Actions to Mitigate Breach Risk		
REVIEWED BY: AZPC Compliance Officer	**REVIEW DATE: 11/08/2019**	**EFFECTIVE DATE: 12/01/2019**
APPROVED BY: Compliance Committee	**APPROVAL DATE:** 11/11/2019	

PURPOSE:

To ensure that Arizona Priority Care (AZPC) applies corrective action 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 AZPC Compliance Plan.

POLICY:

It is AZPC's policy to prevent any violations of non-compliance and immediately correct any violations by issuing corrective actions and/or implementing system changes to ensure that a similar violation does not occur in the future.

PROCEDURE:

To comply with above policy, AZPC will follow the procedure detailed below:

1. Privacy breaches and/or violations of non-compliance are evaluated according to AZPC's Compliance Plan 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, Cyber Security, Model of Care, Cultural and Linguistics, and Injury and Illness, Harassment) in accordance with company policy, and 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 (855-625-7894).
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. HIPAA Risk Assessment Analysis Tool, Fraud, Waste, and Abuse letter).
5. Compliance tools for identifying employee violations and/or to evaluate associated risk include, but are not limited to: surveillance cameras, internet usage reports, witnesses, phone records, HIPAA Risk Assessment Analysis Tool, 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 Business Associate Agreement 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.

DEFINITIONS:

None

REFERENCES:

Heritage Provider Network Policies

APPENDICES:

Compliance Program Location
Incident Notification Log
HIPAA Risk Assessment Analysis Tool
Fraud, Waste, and Abuse Provider Letter Template

DEPARTMENT: Compliance **POLICY TITLE:** CMP08 Actions to Mitigate Risk	Arizona Priority Care™ *One Goal. One Priority. Your Healthcare.*

DOCUMENT REVISION LOG

Date	Document Modification (including deletions)	Page(s)	Location
11/2019	Transfer to AZPC template	All	All