Policy Title	**Breaches of PHI**
Department	**Compliance**
Policy Number	**COMP 21**
Effective Date	**8/1/2019**
Last Revision Date	**3/1/2020**
Health Plan	☑ **AHOC** ☑ **ABC** ☑ **BSOC** ☑ **SFHP** ☑ **HN** ☑ **UNHC** ☑ **BND** ☑ **AETNA**
Line of Business	☑ **Medicare** ☑ **Medi-cal** ☑ **Commercial** Full, part-time, temporary, contract workers/employees

Purpose

The Medical Group has adopted this Response Procedure to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulations, the Joint Commission on Accreditation of Healthcare Organizations Accreditation standards, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. In addition, this Response Procedure will assist the Medical Group in fulfilling its obligation under the DHHS privacy regulations to mitigate damages caused by breach of individual privacy. All personnel of the Medical Group must comply with this policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

Definitions:

Individually Identifiable information: includes name, address, phone number, SS number, email address, or other information that, alone or in combination with other publicly available information, reveals the individual identity

Medical Information: includes electronic data and any information obtained from a provider of healthcare

Policy

This Response Procedure is based on:

- Protecting individually identifiable information and medical information from misuse and set up preventative measures against potential breaches
- Breaches of security, confidentiality, or the Medical Group's policies and procedures may occur despite security and confidentiality protections.
- Early detection and response to such breaches is critical to stop any such breach, correct the problem, and mitigate any harm.
- In appropriate cases, a thorough investigation is necessary to assess the breach, mitigate any harm, determine how to prevent recurrence, and provide a basis for any necessary disciplinary action.

The purpose of responding to and investigating health information breaches, unnecessary PHI collection, and suspected breaches is to as follows:

- Minimize the frequency and severity of incidents.
- Provide for early assessment and investigation before crucial evidence is gone.
- Quickly take remedial actions to stop the breaches, correct the problems, and mitigate damages.
- Implement measures to prevent recurrence of incidents.
- Facilitate effective disciplinary actions against offenders.

It is the responsibility of every staff member to protect and ensure the protection of both identifiable information and medical information from misuse. Individuals detecting or suspecting a breach of health information security or confidentiality must report the breach or suspected breach as specified therein, including a written report to the manager of information systems as soon as possible as specified in the Medical Group's Report Procedure.

Upon receiving the report, the manager of information systems will take the following steps:

- Take any necessary immediate corrective action.
- If the breach appears to involve gross negligence, willful misconduct, or criminal activity of a person or persons holding access privileges,

immediately, in conjunction with the system administrator, suspend that person(s) access pending investigation, including taking all necessary steps to prevent access (removal of user accounts, recovery of keys, and so forth).

- Provide copies of the report with an endorsement as to any corrective action taken, including suspensions of access, and recommendations for future action to all the following people and departments:
    - Chief Executive Officer
    - Information technology
    - Human resources
    - Privacy/Compliance officer
    - Applicable department directors.
    - Others_____.
- The Chief Executive Officer may appoint an investigating officer, who may be the security officer, to conduct an investigation in appropriate cases. Factors to be considered in determining whether an investigation is necessary include the following:
    - Seriousness of the breach.
    - Whether the breach resulted in actual harm.
    - Extent of any harm.
    - Whether the breach has the potential for legal liability.
    - Whether the breach involved gross negligence, willful misconduct, or criminal activity.
    - Whether the breach put patient or other individuals' welfare at risk.
    - Whether there has been a series of similar or related breaches.
    - Whether the suspected offender has committed other breaches.
- The investigating officer will conduct a thorough investigation into all the facts and circumstances of the breach or suspected breach and will provide the Medical Group's Chief Executive Officer a detailed report of the facts and circumstances of the breach including recommendations for corrective and/or disciplinary action.
- All Medical Group personnel will cooperate with any such investigation. Failure to cooperate, failure to furnish required in formation, or furnishing false information may result in employee discipline up to and including termination under the Medical Group's sanction policy. Department directors will ensure that the investigating officer has access to necessary persons and information to conduct a thorough investigation.
- The Chief Executive Officer, the security officer, the investigating officer, and other appropriate personnel will discuss the report and recommendations

and decide on appropriate action to prevent recurrence of the breach, mitigate any harm caused by the breach, and take necessary disciplinary action in accordance with Medical Group's sanction policy.

- Personnel will keep all such reports for not less than six years from the date of the report.

Notification to contracted Health Plans

- In the event of a breach in protected health information (PHI), the Medical Group will follow the requirements by contracted health plans to report on such breach. The Chief Executive Officer or appointed officer, without unreasonable delay and in no case later than 24 hours after the discovery, shall notify in writing, the contracted health plans whose members are impacted by the breach. The notice will include a report of the following, to the extent possible:
    - Names of the individuals whose PHI was involved in the breach
    - Circumstances surrounding the breach
    - Date of the breach and the date of its discovery
    - Information breached
    - Steps taken to investigate the breach, mitigate losses, and protect against future breaches
    - Any steps the impacted individuals should take to protect themselves
    - Contact person who can provide additional information about the breach

Enforcement

All officers, agents, and employees of the Medical Group must adhere to this policy. The Medical Group will not tolerate violations of this policy. Violations of this policy are grounds for disciplinary action up to and including termination of employment and criminal or professional sanctions in accordance with the Medical Group's medical information sanction policy and personnel rules and regulations.