Policy Title	**Breaches of PHI Incident Report**
Department	**Compliance**
Policy Number	**COMP 23**
Effective Date	**8/1/2019**
Last Revision Date	**5/1/2019**
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

CCHCA has adopted this Report Procedure to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health and Human Services ("DHHS") security and privacy regulations, and the Joint Commission on Accreditation of Healthcare Organizations ("JCAHO") 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. All personnel of CCHCA 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.

Assumptions

This Report Procedure is based on the following assumptions:

- Breaches of security, confidentiality, or CCHCA'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.
- All personnel must know how to report breaches and suspected breaches.

Policy

The purpose of reporting health information breaches and suspected breaches is 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 breaches, correct problems, and mitigate damages.
- Implement measures to prevent recurrence of incidents.
- Facilitate effective disciplinary actions against offenders.

It is the policy of CCHCA that all personnel should not only feel free to report breaches, without fear of reprisal, but also understand they have a duty to do so.

CCHCA will not take any adverse personnel or other action against a person who reports actual or suspected breach of security, confidentiality, or CCHCA's policies and protecting the security and confidentiality of health information so long as the report is made in good faith. Making a knowing false report, however, may result in disciplinary action under CCHCA's sanction policy.

Who Should Report?

All employees and others with access to health information must report breaches of security/confidentiality or of CCHCA's policies and procedures protecting the security and confidentiality of health information as specified below.

What Should Be Reported?

Employees and others must report the following:

- Breach of security, defined as any event that inappropriately places health information at risk for unavailability, improper alteration, breach of confidentiality, or other potential harm to patients, staff, CCHCA itself, or others that may result in adverse legal action.
- Breach of confidentiality, defined as the improper disclosure of individually identifiable health information to a person or entity not authorized to receive the information.
- Any violation of CCHCA's policies and procedures relating to the security or confidentiality of patient information.
- Any violation of CCHCA's policies and procedures relating to the proper use of computer and other information systems equipment.

How to Report

The person discovering the breach or suspected breach must institute the reporting procedure as soon as possible after the occurrence of the breach or its discovery. The person discovering the breach must take the following actions:

- Initiate any necessary corrective action. If, for example, a data user detects a burning odor at a workstation, he or she should immediately tum off the power to the system components. If, for example, a data user detects an unauthorized person observing confidential patient data on a computer screen, he or she should cover the screen, turn off the screen, or otherwise prevent the unauthorized person from continuing to view it.
- Notify the fire department or other emergency services if necessary.
- Report the matter to building security if necessary, such as in the case of an unauthorized person who refuses to leave immediately.
- Report the incident to his or her immediate supervisor if the supervisor is available.
- Report the incident to CCHCA's Compliance Officer or Manager of Information Technology.
- As soon as possible, make a written report of the following information:
    a. Person submitting the report.
    b. Date and time of the report.
    c. Date and time of` the incident.
    d. Location of the incident.
    e. Health information resources involved (hardware, software, data).
    f. Persons involved (suspects, witnesses).
    g. Nature of the breach.
    h. Harm, if any, observed.
    i. Any statements made by suspects and witnesses.
    j. Who was notified
    k. Remedial action, if any, taken.
    l. Recommendations for corrective action.
- Such reports are a risk management tool and not a patient care document. No such report may be made a part of a patient's medical record.
- The Compliance Officer must maintain copies of all reports for at least (10) years from the date of the report.

Enforcement

All officers, agents, and employees of CCHCA must adhere to this policy. CCHCA 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 CCHCA's medical information sanction policy and personnel rules and regulations.