# Yakutat Community Health Center
# Security Policy 4.0
# Facility Access Controls

Issue Date: **12-1-2017**
Effective Date: **12-1-2017**
Responsible for Review: **Chief Compliance Officer**
Scheduled Review Date: **12-1-2019**

## 1.0 HIPAA Regulation:

- 164.310(a)(1) *Facility security plan*
- 164.310(a)(1) *Facility access controls*
- 164.310(a)(1) *Access control and validation procedures*
- 164.310(a)(1) *Maintenance records*
- 164.310(a)(1) *Contingency operations*

## 2.0 Policy Purpose:

The intent of this policy is to establish protocols for securing facilities that contain Electronic Protected Health Information (EPHI).

## 3.0 Policy Description:

### 3.1 General

Yakutat Community Health Center (YCHC) shall reasonably safeguard EPHI from any intentional or unintentional use or disclosure. The YCHC shall protect its facilities where EPHI can be accessed.

### 3.2 New or Remodeled Facility in a covered component

When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Compliance Officer to ensure the facility plan components below are compliant with the HIPAA Regulations.

### 3.3 Facility Security Plan

The YCHC shall safeguard the facilities of its covered components and the equipment therein from unauthorized physical access, tampering and theft. The YCHC Compliance Officers shall annually audit covered component facilities to ensure EPHI safeguards are continuously being maintained.

Facility security guidelines for the workforce:

a. Do not share access cards to enter the facility
b. Do not allow other persons to enter the facility by "piggy backing" *(entering the facility by walking behind an authorized person through a door without using a card in the reader)*

c. Do not share hard key access to enter the facility
d. Do not share alarm codes or keypad codes to enter the facility

One or more of the following shall be implemented for all sites that access EPHI:

1. Visitor Access Control: In facilities in which EPHI is available, all visitors shall be escorted and monitored. Each facility shall implement procedures that govern visitor access controls. These procedures may vary depending on the facilities structure, the type of visitors, and where the EPHI is accessible.

2. Metal/Hard Keys: Facilities that use metal/hard keys shall change affected or appropriate key locks when keys are lost or a workforce member leaves without returning the key. In addition, the facility shall have:
   a. Clearances based on programmatic need, special mandated security requirements and workforce member security.
   b. A mechanism to track which workforce members are provided access.

3. Network Closet(s): Every network closet shall be locked whenever the room is unoccupied or not in use. Covered components shall document who has access to the network closets and periodically change the locking mechanism to these closets.

4. Server Room(s): Every server room shall be locked whenever the room is unoccupied or not in use. Covered components shall document who has access to each server room and periodically change the locking mechanism to server rooms. *Remediation Plan: While YCHC does not currently have a locked server room, the new health center facility construction (scheduled for completion in 2019) will include a secure server room.*

5. Alarm Systems: All buildings that have EPHI shall have some form of alarm system that is activated during non-business hours. Alarm system codes may only be provided to workforce members that require this information in order to leave and enter a building. These alarm codes shall be changed at least every six months. *Remediation Plan: While YCHC does not currently have alarm systems in place, the new health center facility construction (scheduled for completion in 2019) will include an alarm system.*

6. Doors: All external facility doors and doors to areas with EPHI shall remain completely shut at all times. It is each workforce member's responsibility to make sure the door that is being entered or exited is completely shut before leaving the door. Sometimes the doors do not completely close by themselves. If a door's closing or locking mechanism is not working, it is every worker's responsibility to notify the facility manager or designee for that facility.

**3.4 Contingency Operations - Emergency Access to Facilities**

Each facility shall have emergency access procedures in place that allow facility access to appropriate persons to access data as well as support restoration of lost data. This

includes a primary contact person and backup person when facility access is necessary after business hours by persons who do not currently have access to the facility.

**3.5 Maintenance Records Policy**

Repairs or modifications to the physical building for each facility where EPHI can be accessed shall be logged and tracked. These repairs are tracked centrally by General Services – Facility Management. The log shall include events that are related to security (for example, repairs or modifications of hardware, walls, doors and locks).

**4.0 Policy Responsibilities:**

4.1 Manager/supervisor Requirements:

1. Take appropriate corrective action against any person who knowingly violates the facility plan
2. Authorize clearances that are appropriate to the duties of each workforce member
3. Notify the security administrator or designee within one business day when a user no longer requires access to the facility
4. Verify that each worker surrenders her/his key upon leaving employment

**4.2 Worker Requirements:**

1. Display their access/security card to demonstrate their authorization to access restricted areas
2. Immediately report lost metal keys
3. Surrender key upon leaving employment

**4.3 Facility Manager/Security Officer or Designee Requirements:**

1. Request and track maintenance repairs
2. Establish and maintain a mechanism for accessing the facility in an emergency
3. Track who has access to the facility
4. Change metal locks when a key is lost or unaccounted for
5. Change the alarm code every six months

**4.4 Security Officer Responsibilities:**

1. Work with General Services and covered components to ensure facilities comply with the HIPAA Security Rule for facility access controls
2. Conduct annual audits of covered component facilities to ensure the facility is secured and the requirements of this policy are being enforced

**5.0 Procedures**

Each covered component shall document written procedures for their facility security plan. Procedures shall be written to address the unique requirements of each facility. An essential part of compliance is to document and implement processes to ensure the safeguards in the facility security plan are being maintained.

Each covered component shall submit new and revised procedures and plans to the Compliance Officer for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the YCHC HIPAA policies and not deviate from the YCHC standard.

**6.0 Definitions**

- Covered Entity: A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

- Business Associate Definition: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

- E/PHI: Electronic/Protected Health Information means individually identifiable health information:
  - Transmitted by electronic media
  - Maintained in electronic media
  - Transmitted or maintained in any other form or medium

AUTHORIZED BY: Rhoda Jensen, Executive Health Director