Yakutat Community Health Center

Security Policy 7.0
Audit 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:

- 164.308(a)(5) *Log-in monitoring*
- 164.308(a)(5) *Information system activity review*
- 164.312(b) *Audit controls*

2.0 Policy Purpose:

The intent of this policy is to provide the authority for workforce members representing the Yakutat Community Health Center (YCHC) IT organizations to conduct a security audit on any computing resource of the YCHC.

Activity reviews provide indications that implemented safeguards are working, or that safeguards are insufficient. Audits may be conducted to:

1. Ensure integrity, confidentiality and availability of information and resources
2. Investigate possible security incidents to ensure conformance to YCHC IT and security policies
3. Monitor user or system activity where appropriate
4. Verify that software patching is being maintained at the appropriate security level
5. Verify virus protection is being maintained at current levels

3.0 Policy Description:

<u>3.1 Log-in Monitoring</u>

YCHC has the right to monitor system access and activity of all workforce members.

To ensure that access to servers, workstations and other computer systems containing EPHI is appropriately secured; the following log-in monitoring measures shall be implemented:

1. A mechanism to log and document four or more failed log-in attempts in a row shall be implemented on each network system containing EPHI when the technology is capable.

2. Log-in activity reports and logs shall be reviewed biweekly at a minimum to identify any patterns of suspicious activity.
3. All failed log-in attempts of a suspicious nature, such as continuous attempts, shall be reported immediately to the Security Officer or designated Compliance Officers for each covered component.
4. To the extent that technology allows, any User ID that has more than four-repeated failed log-in attempts in a row shall be disabled for a minimum of 30 minutes.

3.2 Information System Activity Review – Audit Controls

To ensure that activity for all computer systems accessing EPHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Each fiscal quarter, at a minimum, every application and system administrator or designee shall review audit logs, activity reports or other mechanisms to document and manage system activity.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with EPHI shall be archived.
5. Audit information and audit tools shall be protected from unauthorized access, modification and deletion.

4.0 Policy Responsibilities:

System administrators, Security Officers and/or other Compliance Officers are responsible to implement and monitor audit controls for all systems that contain EPHI.

5.0 Procedures

Each covered component shall submit all new and revised procedures to the Office of HIPAA for approval and ongoing evaluation. The Compliance Officers shall create audit control checklists and logs to assist with, and standardize, the audit function. 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