Yakutat Community Health Center

Security Policy 11.0
Contingency Plan

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)(7) *Contingency plan*
- 164.308(a)(7) *Data backup plan*
- 164.308(a)(7) *Disaster recovery plan*
- 164.308(a)(7) *Emergency mode operation plan*
- 164.308(a)(7) *Testing and revision procedures*
- 164.308(a)(7) *Applications and data criticality analysis*
- 164.310(a)(1) *Contingency operations*

2.0 Policy Purpose:

The purpose of this policy is to establish rules for continuing business without the normal resources of the Yakutat Community Health Center (YCHC).

3.0 Policy Description:

Each covered component shall develop procedures for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains EPHI is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster Recovery Plan
- Emergency mode operation plan

Each of the following plans shall be evaluated and updated at least annually as business needs and technology requirements change.

3.1 Applications and Data Criticality Analysis

1. Each HIPAA covered component shall assess the relative criticality of specific applications and data within the covered component for purposes of developing

its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

2. Each covered component shall identify critical business functions, define impact scenarios and determine resources needed to recover from each impact.
3. The assessment of data and application criticality shall be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

3.2 Data Backup Plan

1. All EPHI shall be stored on network servers in order for it to be automatically backed up by the system.
2. EPHI shall not be saved on the local drives of personal computers.
3. EPHI stored on portable media shall be saved to the network to ensure backup of EPHI data.
4. The YCHC shall conduct daily backups of user-level and system-level information and store the backup information in a secure location. A weekly backup shall be stored offsite.
5. Each covered component shall establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all EPHI.
6. The Data Backup Plan shall apply to all files that may contain EPHI.
7. The Data Backup Plan shall require that all media used for backing up EPHI be stored in a physically secure environment, such as a secure, offsite storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
8. If a non-YCHC offsite storage facility or backup service is used, a written contract shall be used to ensure that the contractor shall safeguard the EPHI in an appropriate manner.
9. Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis to ensure that exact copies of EPHI can be retrieved and made available.
10. Each covered component shall submit its new and revised Data Backup Plan to the Compliance Officers for approval.

3.3 Disaster Recovery Plan

1. To ensure that each covered component can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure or natural disaster effecting systems containing EPHI, each covered component shall establish and implement a Disaster Recover Plan pursuant to which it can restore or recover any loss of EPHI and the systems needed to make that EPHI available in a timely manner. The Disaster Recovery Plan for each covered component shall be incorporated into the YCHC Disaster Recovery Plan.
2. The Disaster Recovery Plan shall include procedures to restore EPHI from data backups in the case of a disaster causing data loss.

3. The Disaster Recovery Plan shall include procedures to log system outages, failures and data loss to critical systems and procedures to train the appropriate personnel to implement the Disaster Recovery Plan.
4. The Disaster Recovery Plan shall be documented and easily available to the necessary personnel at all times, who shall be trained to implement the Disaster Recovery Plan.
5. The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.
6. Each covered component shall submit its new and revised Disaster Recovery Plan to the Chief Compliance Officer for approval

3.4 Emergency Mode Operation Plan

1. Each covered component shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode. Emergency mode operation involves those critical business processes that shall occur to protect the security of EPHI during and immediately after a crisis situation
2. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
3. Each covered component shall submit its new and revised Emergency Mode Operation Plan to the Chief Compliance Officer for approval.

4.0 Policy Responsibilities:

The Office of HIPAA shall oversee the creation, evaluation, testing and update of the various contingency plans described herein.

Each covered component shall submit its new and/or revised procedures and plans to the Office of HIPAA 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.

5.0 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