COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Contingency Plan	**POLICY NO:** 01-297
SECTION: Administration	**EFFECTIVE DATE:** 6-8-16
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Part 164	**PAGE:** 1 of 5
	SUPERSEDES: New Policy
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	**APPROVED BY:** Andrea Kuhlen

PURPOSE: To identify the components of a Contingency Plan.

SCOPE: The information in this document applies to all members of the workforce which includes employees, contract employees, volunteers, trainees, etc., granted access to protected health information (PHI).

NOTES: The Security Officer or his/her designee must ensure that a Contingency Plan containing the components in Sections I through VII below is created, implemented, tested, and updated for each ICBHS facility. The ICBHS Facilities Plan and Disaster Plan, including the components identified below, must be provided to the Security Officer for review and approval to ensure that the minimum Contingency Plan requirements are met.

DEFINITIONS: **Contingency Plan:** A plan for emergency response, backup procedures, and post-disaster recovery, synonymous with disaster plan and emergency plan.

IT: Information Technology

Workforce: Employees, volunteers, trainees, and

other persons whose conduct, in the performance of work for department, whether or not they are paid by the department.

POLICY: The Contingency Plan consists of the following seven components:

I. Application and Data Criticality Analysis

a. The Application and Data Criticality Analysis must identify IT Contingency Plan priorities based on the criticality and sensitivity of the applications and data within the facility. The Applications and Data Criticality Analysis must include:

Identification of the assets (e.g., hardware, software, and applications) utilized by the facility that receive, manipulate, store and/or transmit confidential and/or sensitive information, as well as information necessary to ongoing business operations.

b. Prioritization of applications and data to ensure crucial applications are installed and functional.

II. Data Backup Plan

The Data Backup Plan must ensure that exact copies of critical data are retrievable. The Data Backup Plan must:

a. Identify the backup methods (e.g., full, incremental, or differential backup) and materials (e.g., CD-ROM, magnetic tape, or floppy disks) to be used.

b. Identify the frequency of performing backups based on the criticality analysis.

c. Assign a responsible person(s) to catalog, store, and secure the backups in a suitable container and location for such purpose.

III. Disaster Recovery Plan

The Disaster Recovery Plan must enable the restoration

of lost data in the event of fire, vandalism, systems failure, or other disaster. The Disaster Recovery Plan must:

a. Identify the authorized person(s) for the retrieval, loading, and testing of data backups.

b. Identify processes to retrieve of the latest copy of the facilities' backed-up data from the secure location in the event of data loss. If the necessary data set(s) have not been archived, efforts will be made through formal channels (e.g., retransmission from original sources) to collect the data.

c. Identify the process to load and restore data in the order of predetermined criticality to appropriate components and test to ensure the data restoration was successful.

IV. Emergency Mode Operation Plan

The Emergency Mode Operation Plan must enable ICBHS facilities to continue its operations and business processes in the event of fire, vandalism, systems failure, or other disaster, and safeguards the security of data. The Emergency Mode Operation Plan must be based on the emergency preparedness plan for each ICBHS division and must:

a. Identify the scope including the severity of the emergency (e.g., system only, facility-wide, ICBHS-wide) and the duration of the emergency (e.g., until repair, day, week, month, undetermined).

b. Identify type of recovery (e.g., onsite assistance recovery, remote offsite, disk mirroring) that is required by the scope of the emergency.

c. Identify emergency continuity personnel, including either backup personnel or personnel cross-trained to assure adequate staffing in the event of an emergency.

d. Designate specific roles and responsibilities to initiate and maintain emergency mode operations, including information system and security personnel.

e. Implement the following emergency access control requirements:

1. Determine emergency access control requirements for emergency mode operations and ensure that the access control matrices reflect such requirements.

2. Give users additional privileges in the event of a crisis situation to access information as needed and in accordance with the above emergency mode operation procedures.

V. Command and Control Plan

The Command and Control Plan must establish IT administrative procedures to follow in the event that an emergency occurs. The Command and Control Plan must:

a. Integrate the ICBHS Contingency Plan with existing ITS Contingency Plan to establish command and control in order to support ICBHS emergency management team members who can facilitate the flow of information technology as necessary to users.

b. Develop a telephone call tree to disseminate important information within ICBHS facilities, as necessary.

c. Establish a notification process to notify the appropriate persons within management roles arid the ICBHS facilities in the event any part of the Contingency Plan is executed.

VI. Test and Revision of Contingency Plan

The Contingency Plan must be tested periodically in order to assure the workability of the plan in the event

of a disaster and/or emergency. If testing establishes the need for changes in existing Contingency Plan procedures, then those procedures must be revised.

VII. Workforce Contingency Plan Training

a. ICBHS must train and prepare designated workforce members as necessary regarding the Contingency Plan.