OLIVE VIEW-UCLA MEDICAL CENTER
POLICY & PROCEDURE

NUMBER: 1256
VERSION: 1

SUBJECT/TITLE: **CONTINGENCY PLAN**

POLICY: Olive View-UCLA Medical Center must develop and implement an IT Contingency Plan.

1. The IT Contingency Plan serves as a master plan for responding to IT system emergencies (e.g., fire, vandalism, system failure, and natural disaster) ensuring continuity of operation during an emergency and recovery from a disaster. The IT Contingency Plan includes:

   a. Policies and procedures that address electronically maintained or transmitted Protected Health Information (PHI) and other information.

   b. Application and Data Criticality Analysis – an assessment of the relative criticality of specific electronic information systems and data.

   c. Data backup – A process for retrieving exact copies of data.

   d. Disaster recovery – procedures for restoring any lost data.

   e. Emergency mode of operations – procedures to enable business continuity and protect the security of electronic IT information-during and immediately after an emergency.

   f. Command and control – the provision of IT administrative direction in the event an emergency occurs.

   g. Testing and revision procedures – to perform periodic testing and revision of the IT Contingency Plan.

   h. Workforce IT Contingency Plan training – to train and prepare designated workforce members regarding the IT Contingency Plan.

2. The Contingency Plan will be tested as set forth in paragraph VI of the procedure below, Testing and Revision of Contingency Plan at least once every year and updated as necessary.

3. Olive View-UCLA Medical Center CIO/designee is responsible for reviewing and updating the IT Contingency Plan. IT Contingency Plans may be periodically enhanced as appropriate to further Olive View-UCLA

Medical Center's business purposes. All IT Contingency Plans, including the components identified in paragraph 1 above and any revisions, must be provided to the DISO for review and approval to ensure that the minimum IT Contingency Plan requirements are met.

PURPOSE: To define Olive View-UCLA Medical Center Information Technology (IT) Contingency Plan.

DEPARTMENTS: All

DEFINITIONS: **CONTINGENCY PLAN** – A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan.

DISASTER RECOVERY – A plan for the restoration of lost data, or the reconciliation of conflicting or erroneous data, after a system failure due to natural or manmade disaster.

INFORMATION TECHNOLOGY (IT) – A term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, personal health information, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).

OVERVIEW: Olive View-UCLA Medical Center IT Contingency Plan for Olive View-UCLA Medical Center must ensure the security (confidentiality, integrity and availability) of Protected Health Information (PHI) and other confidential information in the event of any disruption, disaster or other emergency by planning for the recovery and continued operation of electronic information systems.

In accordance with the priority determined in the criticality analysis, disaster recovery plan focuses on the sequences and method of recovering Information Systems, and the data they hold, from the data secured in storage by the backup plan. In contrast, the emergency mode operation plan assures the day-to-day operation of the Olive View-UCLA Medical Center during the emergency with the minimum required data set, with or without a full recovery of the system.

PROCEDURE: Olive View-UCLA Medical Center CEOs/Directors are responsible for approving prioritization of the critical information systems to ensure the ranking accurately reflects the relative criticality of the Department's business functions.

The Olive View-UCLA Medical Center CIO/designees must ensure that an IT Contingency Plan containing the components in I through VI below is created, implemented, tested, and updated for each Olive View-UCLA Medical Center facilities. The Olive View-UCLA Medical Center IT Contingency Plans, including the components identified below, must be provided to the DISO for review and approval to ensure that the minimum IT Contingency Plan requirements are met.

I. **Application and Data Criticality Analysis** (Appendix I – Olive View-UCLA Medical Center IT Contingency Plan Guideline, Section 1)

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 Olive View-UCLA Medical Center. The Application and Data Criticality Analysis must include:

A. Identification of the assets (e.g., hardware, software, and applications) utilized by the Olive View-UCLA Medical Center that receive, manipulate, store and/or transmit confidential information, as well as information necessary to ongoing business operations.

B. Prioritization of application and data based on the Criticality Score and Sensitivity Score found in the Olive View-UCLA Medical Center Master Security Management Report in Olive View-UCLA Medical Center policy "Security Management Process: Risk Management"

II. **Data Backup Plan** (Appendix I – Olive View-UCLA Medical Center IT Contingency Plan Guideline, Section 2)

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

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, and the frequency of performing backups based on the criticality analysis.

B. Assign a responsible person(s) to manually backup the data sets as determined, or configure the backup to be done automatically by available tools. The backups will be inspected and tested to ensure that their contents are exact copies of the data-archived, and that they are restorable.

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

D. Monitor and track storage and removal of backups; ensure all applicable access controls are enforced.

E. Track the archive requirements for each backed up data set; ensure they are maintained for the appropriate time period.

F. Test the Data Backup plan as set forth in section VI below.

III. Disaster Recovery Plan (Appendix I – Olive View-UCLA Medical Center IT Contingency Plan Guideline, Section)

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 include the following steps:

A. Assign and provide access rights to an authorized person(s) for the retrieval, loading and testing of data backups.

B. Retrieval of the latest copy of the Olive View-UCLA Medical Center's backup 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. Load the retrieved data in the order of pre-determined criticality (especially with regard to the availability attribute), to appropriate components (in accordance with applicable access control policies) and test to ensure the data restoration was successful.

D. Test the Disaster Recovery plan as set forth in section VI below.

IV. Emergency Mode Operation Plan (Appendix I – Olive View-UCLA Medical Center IT Contingency Plan Guideline, Section 4)

The Emergency Mode Operation plan must enable the Olive View-UCLA Medical Center 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 criticality analysis for each IT Information System and must include the following steps:

A. Identify the scope including the severity of the emergency (e.g., system only, Olive View-UCLA Medical Center-wide) and the duration of the emergency (e.g., until repair, day, week, month, undetermined).

B. Identify type of recovery (e.g., hot site, warm site, cold site, disk monitoring) 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 in accordance with the Emergency Access Control Procedure in Olive View-UCLA Medical Center policy "System Access Control".

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.

F. Test the emergency mode operation procedures as set forth in section VI below.

V. Command and Control Plan (Appendix I – Olive View-UCLA Medical Center IT Contingency Plan Guideline, Section 5)

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

A. The Olive View-UCLA Medical Center CIO/designee must integrate the Olive View-UCLA Medical Center IT Contingency Plan with existing Olive View-UCLA Medical Center Contingency Plan to establish command and control in order to support emergency management team members who can facilitate the flow of information as necessary to users.

B. Develop a call tree to disseminate important information within Olive View-UCLA Medical Center as necessary.

C. Olive View-UCLA Medical Center must have in place a notification process to notify the appropriate persons within Olive View-UCLA Medical Center, in the event any part of the IT Contingency Plan is executed.

VI. **Testing and Revision of Contingency Plan** (Appendix I – Olive View-UCLA Medical Center IT Contingency Plan Guideline, Section 6)

The IT 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 IT Contingency Plan procedures then those procedures must be revised.

A. Conduct one or more of the following exercises to test the IT Contingency Plan (including backup, disaster recovery, and emergency mode operation plans):

1. Tabletop exercise of response to specific scenarios

2. Technical Restoration activities

3. Supplier and/or services tests

4. Complete drills of data backup plan, disaster recovery plan and the emergency mode operations plan.

B. Revise the IT Contingency Plan to address any deficiencies discovered during the testing activities. Focus on improvements to role and responsibility definitions, processes, practices, and strategies.

C. Revise the IT Contingency Plan as needed if there are important changes involving personnel, contact information, suppliers, legislation or business risks, processes or strategies.

D. Annually conduct one or more of the exercises to test the IT Contingency Plan as set forth in paragraph A. above or when there are significant changes to the environment.

VII. **Workforce IT Contingency Plan Training** (Appendix I – Olive View-UCLA Medical Center IT Contingency Plan Guidelines, Section 7)

Olive View-UCLA Medical Center facilities must train and prepare designated workforce members as necessary regarding the IT Contingency Plan.

AUTHORITY: 45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(7)(i) and (ii)

Board of Supervisors Policies:

6.100, Information Technology and Security Policy
6.103, Countywide Computer Security Threat Response
6.107, Information Technology Risk Assessment

References: Olive View-UCLA Medical Center Policy, "Security Management Process: Risk Management" Olive View-UCLA Medical Center Policy, "System Access Control"	
Approved by: Rima Matevosian (Chief Medical Officer)	Date: 05/03/2010
Review Date: 7/05, 05/30/2019	Revision Date:
Next Review Date: 05/30/2022	
Distribution: Olive View Hospital-Wide Policies	
Original Date: 07/01/2005	