County of Los Angeles **Department of Health Services**

OLIVE VIEW-UCLA MEDICAL CENTER
INFORMATION SYSTEM DEPARTMENTAL
POLICY & PROCEDURE

NUMBER: 1259
VERSION: 1

SUBJECT/TITLE: **INFORMATION TECHNOLOGY (IT) CONTINGENCY PLAN**

POLICY: ValleyCare must develop and implement an IT Contingency Plan as outlined in DHS Policy#935.07 INFORMATION TECHNOLOGY (IT) CONTINGENCY PLAN

PURPOSE: To define the ValleyCare Information Technology (IT) Contingency plan according to DHS Policy#935.07 INFORMATION TECHNOLOGY (IT) CONTINGENCY PLAN.

OVERVIEW: The ValleyCare IT Contingency plan 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 DHS Policy#935.07 INFORMATION TECHNOLOGY (IT) CONTINGENCY PLAN.

DEPARTMENTS: **INFORMATION SYSTEMS**

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).

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

PROCEDURE: ValleyCare CEO is 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 ValleyCare CIO/designee must ensure that an IT Contingency Plan is created, implemented, tested, and updated for the ValleyCare/Olive View-UCLA Medical Center System including components I through VI outlined in the procedures of DHS Policy#935.07 INFORMATION TECHNOLOGY (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
Policy No. 6.100, "Information Technology Security Policy
Policy No. 6.103, "Countywide Computer Security Threat Response
Policy No. 6.107, "Information Technology: Risk Assessment

References: DHS Policies: 935.01 Security Management Process: Risk Management 935.14 System Access Control	
Approved by: Susan Aintablian (Chief Information Officer)	Date: 06/01/2010
Review Date: **11/12/2016**	Revision Date:
Distribution: Information Systems	
Original Date: 06/01/2010	