Current Status: *Active*		**PolicyStat ID:** *5019608*
	Effective Date:	*4/20/2005*
	Review Date:	*7/2/2018*
	Revised Date:	*7/2/2018*
	Next Review:	*7/1/2021*
	Owner:	*Ann Chang: Dir*
	Policy Area:	*Compliance*
	Reference Tags:	
Ronald Reagan UCLA Medical Center	**Applicability:**	*Ronald Reagan UCLA Medical Center* *Ambulatory Care - UCLA* *Resnick Neuropsychiatric Hospital* *Santa Monica UCLA Medical & Orthopaedic* *UCLA Health*

Backup and Contingency Plans (Disaster Recovery) Policy, HS 9458

PURPOSE

The purpose of this policy is to describe the backup and contingency plans, including disaster recovery planning, that will be implemented to ensure that Restricted Information can be accessed during an emergency and to ensure the availability of Restricted Information for the patient care and business functions of UCLA Health Sciences in the event of unexpected data loss and/or damage.

SCOPE

This Policy applies to all faculty, staff, employees, students, trainees, and volunteers of the Ronald Reagan UCLA Medical Center, the Santa Monica UCLA Medical Center and Orthopaedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics and the David Geffen School of Medicine at UCLA (hereafter referred to as "UCLA Health Sciences").

In addition, it applies to suppliers, contractors and other non-workforce members who are allowed access to UCLA Health Sciences Electronic Information Resources or Restricted Information and to any devices, including personally owned devices that store Restricted Information.

POLICY

UCLA Health Sciences shall implement processes and procedures to ensure that systems and data containing Restricted Information remain available for patient care and business functions in the event unexpected factors cause temporary unavailability of Restricted Information. Plans must include processes to create backups of original source Restricted Information.

Plans must address both temporary unexpected loss of power, power surges or other situations which can cause damage to computer resources and data, and processes to restore systems in an emergency situation, such as a natural disaster or malware compromises, that may render resources unavailable for a period of time. UCLA Health Science's disaster recovery plans shall be tested on a periodic basis or in response to major changes in the working environment. Departments must also implement contingency plans to ensure that critical

operations can continue during periods of temporary loss of computer infrastructure.

Disaster recovery and contingency plans shall address, at a minimum, processes to:

A. Create, archive and restore backup copies of data containing Restricted Information or other mission critical information

B. Restore applications and systems

C. Obtain or restore hardware equipment

D. Periodically test data restoration

E. Dispose of and/or recycle media and equipment containing Restricted Information or other mission critical information

F. Implement down-time procedures to operate temporarily without computer resources

PROCEDURE

I. **Data Backup and Archival Procedures**

A. Backup copies of **original source** Restricted Information or other mission critical information must be created and updated on a regular basis. The frequency of the backup shall be determined by the frequency with which the information is modified and/or updated, and the criticality of the data for ongoing patient care and business functions.

B. The backups and archives can be stored on:

i. Removable media (e.g., magnetic tape, external hard drives, DVD/CD, etc.)

ii. Network file servers if the data stored on the servers are backed up on a regular schedule and the archival media is stored in a safe, secure environment. (For example, the network file servers maintained by UCLA Health IT are acceptable for backup retention.)

iii. Multiple servers simultaneously (servers should be maintained at separate locations)

iv. Virtual machines

v. Cloud services that have prior approval for use from the Office of Compliance Services - Information Security

C. In the event of damage or malfunction of any system, backup media or alternative data stores must be accessible within a reasonable period of time in order to provide timely access to Restricted Information or other mission critical information for patient care or other immediate needs.

D. Backups of Restricted Information on removable media must be encrypted. (*See*: HS Policy No. 9453-C, "*Device and Removable Media Encryption*.")

E. Backups of Restricted Information stored on servers, virtual servers and Cloud services should be encrypted whenever possible.

F. When removable media is discarded, it should either be overwritten or destroyed, eliminating all possibility that any Restricted Information could be read. (*See*: HS Policy No. HS 9456, "*Physical Security of Restricted Information*.")

G. When system hardware or backup media is recycled, transferred to another user or discarded, all storage devices containing Restricted Information records must be overwritten, rendering all Restricted Information records unreadable. (*See*: HS Policy No. HS 9456, "*Physical Security of Restricted Information*.")

H. For multi-user systems, the backup logs should be periodically reviewed by the appropriate supervisor or manager to ensure that backup processes are complete and working correctly.

I. Backup copies should be stored in a physically separate location from the original data source that would likely allow for the recovery of the information should a reasonably anticipated disaster occur (earthquake, fire, flood, etc).

J. Off-line copies of backups of critical data must be created and kept up to date as on-line backups can be destroyed or corrupted by malware such as ransomware.

K. The appropriate Agreements to safeguard the confidentiality, integrity and availability of backups must be in place before Restricted Information may be stored by any third party. (*See*: HS Policy No. 9430, "*Business Associates*," and HS Policy No. 9451, "*Use of Electronic Information*."

II. **Disaster Recovery and Contingency Plans**

UCLA Health Sciences shall ensure that business continuity planning includes measures to recover from a disaster that renders resources unavailable for a period of time. Disaster recovery plans must be tested on a periodic basis or in response to major changes to the working environment.

A. Restricted Information and other mission critical information should be archived ("backed up") as described in Section 1 above.

B. Current copies of the archival media should be stored at a remote location that is unlikely to be affected by a local disaster. This media would be used to retrieve the Restricted Information or other mission critical information in the event that the system or local archival media is destroyed.

C. In addition to data recovery, processes and procedures must be in place to ensure that applications can be restored in the event of an emergency. Plans can include

i. Creating backup copies of systems where the application runs;

ii. Storing a copy of the application on a central network server;

iii. Maintaining a copy of the application locally within the department; and/or

iv. Completing a contractual agreement with the vendor to obtain a copy of the application from them.

D. A contingency plan or "Down-time Procedures" must be prepared by each UCLA Health Sciences department that specifies the procedures to be implemented in order to function during temporary loss of computer infrastructure such as during a disaster situation. Plans should allow for facility access by IT staff for data restoration.

E. UCLA Health Science's disaster recovery plans must undergo periodic testing and revised as appropriate.

III. **Enforcement**

Failure to follow any provisions of this policy may result in disciplinary action, up to and including termination.

IV. **Policy Exceptions**

Any exceptions to this policy must be for a valid patient care or business reason and must be approved by the Chief Compliance Officer or his/her designee. The Chief Compliance Officer or designee will consult with the appropriate business, leadership and IT groups in evaluating any proposed exceptions. Exceptions may be requested by submitting an exception request form.

V. **Questions**

Contact your IT Support group for information on how to perform backups or on the disaster recovery and

contingency plans for your area. Contact the Office of Compliance Services - Information Security, InfoSecAll@mednet.ucla.edu, if you have any questions on this policy.

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164
California Medical Information Act, California Civil Code Section 56 *et seq.*
Information Practices Act of 1977, California Civil Code Sections 1798.29 and 1798.82
California Health and Safety Code Sections 1280.15 and 130203
University of California Business and Finance Bulletin IS-3, Electronic Information Security
University of California Electronic Communications Policy (ECP)

CONTACT

Chief Privacy Officer, Compliance Office
Chief Information Security Officer, Compliance Office

REVISION HISTORY

Approved:	February 22, 2006
Effective Date:	April 20, 2005
Revised Date:	November 2005; June 21, 2007; May 30, 2008, March 31, 2011, June 29, 2018

APPROVAL

Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010

Johnese Spisso, RN, MPA
President UCLA Health
CEO UCLA Hospital System

Christopher Tarnay, M.D.
Chief of Staff
Ronald Reagan UCLA Medical Center

Roger M. Lee, M.D.
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic hospital

Laurie R. Casaus, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA

Appendix I – Definitions

"Electronic Information Resources" includes, but is not limited to, computer equipment (servers, workstations, laptops and other portable computers), online services, medical devices, mobile devices (tablets ,smart phones, digital cameras, etc.), applications (Electronic Health Record, email, databases, other software), storage media (USB drives, DVDs, CDs, magnetic tape, memory cards), and networks.

"Protected health information" or "PHI" is any individually identifiable health information, in any form or media, whether electronic, paper, or oral. "Individually identifiable" means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, genetic or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes medical information; patient billing and health insurance information; and applies to a patient's past, current or future physical or mental health or treatment.

"Electronic Protected Health Information" or "ePHI" is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

"*Personal Information (PI)*" as used in this policy means either of the following:

A. An individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted:
    1. social security number,
    2. driver's license number or California identification card number,
    3. account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account,
    4. medical information, or
    5. health insurance information, or
    6. information or data collected through the use or operation of an automated license plate recognition system as defined in the California Civil Code §1798.90.5; or
B. A user name or email address, in combination with a password or security question and answer that would permit access to an online account

"***Medical Information***" means any individually identifiable information, in either electronic or physical form, regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and which may be in the possession of or derived from a health care provider, health care service plan, pharmaceutical company or contractor.

"***Health Insurance Information***" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

"Restricted Information" (as defined by UC Policy IS-3, Electronic Information Security) describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. This includes Personal Information, PHI and ePHI as defined in this section but could also include other types of information such as research data.

Attachments:

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval	Johnese Spisso: Ceo Med Ctr [MW]	7/2/2018

Step Description	Approver	Date
Administration Approval	Christopher Tarnay: Hs Assoc Clin Prof-Hcomp [MW]	7/2/2018
Administration Approval	Roger Lee: Hs Clin Prof-Hcomp [MW]	7/2/2018
Administration Approval	Laurie Casaus: Hs Assoc Clin Prof-Hcomp [MW]	7/2/2018
Executive Medical Boards - MSEC, RNPH PSEC, SMEMB	M. Lynn Willis: Mgr	7/2/2018
Hospital System Policy Committee Chair	M. Lynn Willis: Mgr	6/21/2018
Hospital System Policy Committee	M. Lynn Willis: Mgr	6/21/2018
	Ann Chang: Dir	6/2/2018

Applicability

Ambulatory Care - UCLA, Resnick Neuropsychiatric Hospital, Ronald Reagan UCLA Medical Center, Santa Monica UCLA Medical & Orthopaedic, UCLA Health