Current Status: *Active*		**PolicyStat ID:** *4015540*
	Effective Date:	*4/8/2003*
	Review Date:	*9/29/2017*
	Revised Date:	*9/29/2017*
	Next Review:	*9/28/2020*
	Owner:	*Chloe Ghoogassian: Spec*
	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*

Protection of Confidential Patient Information (Protected Health Information (PHI)), HS 9401

PURPOSE

This policy sets forth guidelines for protecting and maintaining the confidentiality of individually identifiable patient health information (referred to hereafter as "Protected Health Information" or "PHI") as required by the federal Health Insurance Portability and Accountability Act of 1996 (the "Privacy Rule") and California law.[1]

SCOPE

This policy applies to the UCLA Health System and David Geffen School of Medicine at UCLA (hereafter referred to as "UCLA Health").

DEFINITIONS

"Protected health information" or "PHI" is any individually identifiable health information, in any format, including verbal communications. "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, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes 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 is an individual's first name or first initial and last name combined with any one of the following:

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.

"*Medical Information*" means any 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. Medical information and health insurance information for patients are also considered to be PHI.

"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.

"Disclosure" is the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

"Health Care Operations" covers a broad range of activities such as quality assessment, patient education and training, student training, contracting for health care services, medical review, legal services, auditing functions, compliance, business planning and development, licensing and accreditation, business management and general administrative activities.

"Payment" can be defined as activities related to being paid for services rendered. These include eligibility determinations, billing, claims management, utilization review, etc. It also includes using debt collection and location agencies.

"Treatment" under the Privacy Rule is defined to include all the preventive, diagnostic, therapeutic, rehabilitation, maintenance and palliative care provided to an individual as well as the provision, coordination, and management of health care and related services by one or more health care providers, including the coordination of management of health care by a health care provider with a third party, consultation between health care providers relating to patient, or the referral of a patient for health care from one provider to another.

"Use" means the sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains such information.

"Workforce" means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Health, is under the direct control of UCLA Health or the Regents of the University of California, whether or not UCLA Health pays them. The Workforce includes employees, medical staff, and other health care professionals, agency, temporary and registry personnel, and trainees, housestaff, students and interns, regardless of whether they are UCLA trainees or rotating through UCLA Health facilities from another institution.

POLICY/PROCEDURE

I. **Protection of Individually Identifiable Health Information (PHI)**

Members of the UCLA Health Workforce may not disclose, share, or otherwise use any individually identifiable health information except for Treatment, Payment and Health Care Operations (referred to

hereafter as "TPO") unless expressly authorized by the patient or otherwise permitted or required by law.

II. **Classification of PHI Information**

All information contained in patient medical and billing records is confidential regardless of format (i.e., print medium, audio recording, electronic display or storage). These confidentiality protections extend not only to the patient's medical record, but also to information from the record. Thus, abstracts of charts, medical record numbers, diagnoses, case histories, or descriptions of medical procedures that include or refer to the patient's name, social security number, or other identifying information, as well as information orally communicated about a particular patient, must be maintained as confidential PHI.

In addition, special laws govern mental health, substance abuse and HIV test result information. Questions regarding the release of sensitive medical information should be referred to the Office of Compliance Services - Privacy or Health Information Management Services.

III. **Notice of Privacy Practices**

The Privacy Rule requires that providers such as UCLA Health System give patients detailed information about their privacy practices. The University's "Notice of Privacy Practices" shall be given to all UCLA Health patients upon admission or, in the case of outpatients, at the time of service, as further described in HS Policy No. 9411, *"Notice of Privacy Practices."*

All uses and disclosures of PHI by UCLA Health System and its Workforce must be consistent with the Notice of Privacy Practices.

IV. **Authorization to Use PHI**

The Privacy Rule requires providers to obtain a written authorization from an individual before using or disclosing a patient's PHI for purposes other than for TPO. UCLA Health s policy and procedures regarding patient authorizations are set forth in HS Policy No. 9412, *"Authorization for Use/Disclosure of PHI."*

V. **Patient Access to PHI**

The Privacy Rule gives an individual (or that person's personal representative) the right of access to inspect and obtain a copy of the individual's own PHI. Providers may deny an individual access to his or her information under certain circumstances only if specified procedures are followed.

All requests from patients for information from medical records should be referred to or coordinated with the Health Information Management Services. (See: HS Policy No. 9413, *"Patient Requests to Access and Receive Copies of PHI in Any Format, Including Electronic."*)

VI. **Restrictions on the Use of PHI**

The Privacy Rule and California law generally allow a provider to use or disclose PHI to carry out TPO. An individual, however, has the right to request that providers restrict their use or disclosure of PHI to carry out TPO – that is, a patient may request that the provider voluntarily agree not to use or disclose PHI in a way that the law would otherwise allow. The Privacy Rule also gives individuals the right to request restrictions on the information that may be released to family or friends.

UCLA Health's policy and procedures regarding how patients may restrict the use of their PHI is set forth in HS Policy No. 9414, *"Request for Special Restriction on Use or Disclosure of PHI."*

VII. **UCLA Health Workforce (Employee) Responsibilities to Maintain Confidentiality of PHI**

All members of the UCLA Health Workforce are responsible for maintaining the security and confidentiality of PHI on behalf of UCLA Health patients. This responsibility includes both the physical (electronic or paper) record and all information contained in or derived from the medical record, including information disclosed or transmitted orally.

A. **Minimum Necessary**

When using or disclosing PHI, or when requesting PHI from another entity, a Workforce member must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. This requirement does not apply to:

i. Disclosures to, or requests by, a health care provider for treatment;

ii. Uses or disclosures made to the individual, as permitted or required;

iii. Uses or disclosures made pursuant to an authorization;

iv. Disclosures made to the Secretary of the Department of Health and Human Services pursuant to an investigation or compliance review; or

v. Other uses or disclosures that are required by law and are compliant with the requirements of the law.

Note: If the request for PHI constitutes a use of information (for example, the sharing of information between two UCLA Health System physicians), the minimum necessary provision still applies.

B. **Workforce Access to PHI**

All members of the UCLA Health Workforce should only access and use PHI ***as necessary for their job functions.*** Repeating or in any way disseminating patient information, either by oral communication or in writing, except as permitted herein or required by law, is considered an unauthorized release of medical information and is a serious offense which may have personal civil and/or criminal liability. Violation of this policy constitutes ground for disciplinary action up to and including termination. (*See*: HS Policy No. 9421, *"Workforce Access to and Use of PHI"* and HS Policy No. 9461*, "Privacy and Information Security Sanction.*")

VIII. **Release of PHI to Third Parties**

A. **Requests for PHI by Outside Entities**

UCLA Health receives numerous requests for copies of medical records on a daily basis from outside entities such as health plans, law enforcement agencies, licensing and regulatory agencies, attorneys, etc. Because of the specific accounting and disclosure requirements imposed by HIPAA, all copying of medical records for release to third parties or agencies must be completed by, or coordinated with, the Health Information Management Services (HIMS) Department.

For example, when releasing PHI to third parties, except for purposes of TPO and those other instances in which the accounting requirements do not apply (i.e., disclosures pursuant to patient written authorization) as stated in the HIPAA Privacy Rule, UCLA Health is required to document all of the following:

i. The date of the disclosure;

ii. The name of the entity or person who received the PHI and the address of such entity or person (if known);

iii. A brief description of the PHI disclosed;

iv. The name of the individual and/or department who completed the disclosure; and

v. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the patient's authorization for such disclosure.

In addition, PHI records shall be screened prior to their release to ensure that: (1) only the minimum necessary information is released; and (2) no privileged information (e.g., attorney-client, peer-review information) is released except as permitted or required by law.

The policies and procedures regarding the release of PHI to third parties are set forth in HS Policy No. 6422, "*Disclosure of Protected Health Information ("PHI") to Third Parties*."

B. **Mandatory Reporting Requirements**

Although a patient has the right to refuse to disclose and to prevent others, including physicians, from disclosing confidential communications between the patient and his/her physicians, there are certain laws, which require or permit a provider to disclose patient records without the patient's written authorization. These circumstances, which are outlined in the Notice of Privacy Practices (*See*: HS Policy No. 9411, "*Notice of Privacy Practices*"), include, but are not limited to:

i. Public health activities that involve safety or communicable disease;

ii. Reporting victims of abuse, neglect, or domestic violence;

iii. Judicial and administrative proceedings;

iv. Law enforcement purposes;

v. Organ and tissue donations;

vi. National security and intelligence activities;

vii. Workers' compensation; or

viii. Requests related to decedents.

(*See also*: HS Policy No. 9010, "*Mandatory Reporting*.")

C. **Mental Health, Substance Abuse and HIV Test Result Information**

Special laws govern mental health, substance abuse and HIV test result information. Questions regarding the release of sensitive medical information should be referred to the Office of Compliance Services - Privacy or Health Information Management Services.

D. **Psychotherapy Notes**

Psychotherapy notes receive stricter treatment under the Privacy Rule than other types of PHI. Psychotherapy notes are narrowly defined under the Privacy Rule to include notes by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private, group, joint or family counseling session which are separated from the rest of the individual's medical record, but exclude certain records.

Prior to releasing any psychotherapy notes without a patient authorization, an employee should first consult with either the Office of Compliance Services - Privacy or the HIMS Department.

IX. Privacy Requirements Relating to Research

Research is not considered to be a part of TPO under the Privacy Rule, except for certain studies related to health care operations, such as quality assurance and utilization management activities. Consequently, the use or disclosure of PHI for research purposes requires either: (1) a written authorization from the individual about whom the information is collected; (2) a waiver of authorization from UCLA Health's Institutional Review Board (IRB); or (3) the satisfaction of another research exception under the Privacy Rule. For further guidance on the privacy requirements relating to research, see HS Policy No. 9440, "*Release of Protected Health Information for Research Purposes."*

A. De-Identified Information

According to the Privacy Rule, health information that does not identify an individual (referred to as "de-identified information") is generally not considered PHI and may be disclosed without the patient's authorization. In order to de-identify PHI, UCLA Health System must remove all eighteen of the HIPAA identifiers specified in the Privacy Rule, In addition, prior to using any such de-identified information for research purposes, there must be no means to re-identify the data by the recipient of the de-identified data set.

The specific requirements that must be met in terms of "de-identifying" data in accordance with the Privacy Rule are set forth in HS Policy No. 9440, *"Release of Protected Health Information for Research Purposes."*

B. Limited Data Sets

The Privacy Rule permits the use and disclosure of a limited data set of information for research purposes without patient authorization provided certain requirements are met, including the entering into a Data Use Agreement with the recipient of the information. (*See*: HS Policy No. 9440, "*Release of Protected Health Information for Research Purposes.*")

X. Disclosure to Business Associates

The Privacy Rule requires providers to enter into a written agreement with certain third parties (individuals or entities) that provide services and functions on behalf of UCLA Health System which involve using, accessing, disclosing, or maintaining PHI. These third parties are referred to in the Privacy Rule as "business associates." (*See*: HS Policy No. 9430, "*Business Associates.*")

XI. Marketing

In general, PHI may not be disclosed for marketing purposes without the patient's authorization. If the marketing involves direct or indirect payment to UCLA Health System from a third party, the authorization form that the individual signs must include a statement that UCLA Health received payment for using and/or disclosing PHI for marketing purposes. The requirements for a valid authorization form, and the exceptions to the general rule regarding disclosure of PHI for marketing purposes, are further described in HS Policy No. 9470, *"Use of Protected Health Information (PHI) for Marketing Purposes.*"

XII. Fundraising

UCLA Health System may use or disclose limited PHI to a Business Associate (see Section X., above) or to an institutionally-related foundation to raise funds for its own benefit, provided the PHI used or disclosed must be limited to demographic information and the dates of health care provided to the individual. Demographic information includes the individual's name, age, gender, insurance status, address and other contact information. UCLA Health System must obtain the individual's prior written authorization to use or disclose any other information (such as the treating or referring physician, the department or practice area, illness or treatment) for fundraising purposes. Since only the individual's demographic information may be used, reports cannot be generated for fundraising purposes from an information system using non-demographic information fields, such as physician, medical condition or clinical department.

In addition, all fundraising materials sent to an individual must describe, in a conspicuous place, how the individual can opt out of receiving further fundraising communications. (*See*: HS Policy No. 9471, *"Use of Protected Health Information (PHI) for Fundraising Purposes.*")

XIII. **Media Inquiries**

Both California law and the Privacy Rule restrict the amount of information that may be provided to the media without the patient's authorization. In general, if the patient has not requested that information be withheld, UCLA Health System may release the condition and location of an inpatient, outpatient, or emergency patient, but only if the inquiry specifically contains the patient's name. No information can be given if a request does not include the patient's name or if the patient has requested that information be withheld.

A patient's condition may only be described in general terms that does not communicate specific medical information about the individual. For example, "undetermined," "good," "fair," "serious," "critical," or "deceased." All inquiries from the media should be referred to the UCLA Health System Media Relations Department. For further guidance on responding to media inquiries, see HS Policy No. 9472, "*Permissible Disclosures of PHI to the Media and the Public.*"

XIV. **Safeguards to Protect PHI**

In addition to protecting the privacy of a patient's health information by complying with regulations regarding use and disclosure of PHI, Workforce members are responsible to protect PHI with reasonable physical, electronic and administrative safeguards. It is the responsibility of all Workforce members to secure PHI that they have access to or are using to complete assigned responsibilities.

Reasonable safeguards are to be used at all times to ensure that confidential information is not disclosed to individuals who are not authorized to receive the information and to minimize incidental disclosures of PHI.

A. **Physical Safeguards**

Each Workforce member is responsible to protect the physical security of the PHI he/she is using, accessing or maintaining in his/her work area, including but not limited to:

i. Ensuring that PHI is not readily visible to visitors or to the public;

ii. Maintaining charts in designated secure areas and not leaving charts unattended in areas to which the public has access;

iii. Locking areas in which there are medical and billing records at the end of the day or when no staff are in the area;

iv. Never taking paper PHI records of any kind offsite (i.e. home) unless doing so is approved by the individual's supervisor through a documented and auditable process;

v. Checking that all PHI is removed upon leaving conference rooms and other meeting locations and the unwanted materials are properly disposed (i.e. shredded); Taking reasonable measures (i.e. lower voices, draw curtains) to provide auditory privacy to individuals in areas where interviews or other conversations including PHI are being conducted and have the potential to be overheard. Examples of such situations would include:

   a. Conversations among care givers that involve patients;

   b. Discussion of a patient's condition or lab tests with the patient, either in person or over the phone; and/or

   c. Discussing a patient's condition during teaching rounds within UCLA Health System;

vi. Positioning computer screens so that the information is not visible to passersby;

vii. Leaving minimal information for patients on answering machines and voice mail;

viii. Locating printers and fax machines in secure areas;

ix. Retrieving and distributing faxed PHI in a timely manner; and

x. Using professional judgment when calling out patient names in the waiting room areas.

xi. At times, minimally necessary information may be displayed and incidentally available in patient treatment areas in the following circumstances:

   i. Information related to the patient's treatment and condition supports patient safety;

   ii. Information is displayed in patient treatment areas to support staff safety; and/or

   iii. Workforce members continue to use physical safeguards to protect all PHI.

B. **Electronic Safeguards**

Workforce members are responsible for ensuring compliance with safeguards to protect electronic information including but not limited to:

i. Not sharing passwords for computer systems;

ii. Not maintaining passwords in locations where they can be obtained and used by others (i.e. post-it notes on computer monitors, stored in a rolodex, placed under computer keyboards); and

iii. Using time out functions or locked screen savers to auto-log out of computer functions when not in use.

Also see HS Policy No 9453-C, "*Storage and Use of Restricted Information on Mobile Devices and Removable Media*."

C. **Administrative Safeguards**

i. Departmental managers are responsible for ensuring that Workforce members under their direction comply with requirements to secure PHI and for providing education and training to Workforce members regarding these requirements.

ii. Workforce members who are responsible for maintaining both PHI and non-PHI must assure that if the data is co-mingled, it is all maintained consistent with HIPAA standards or the data must be maintained in separate formats.

XV. **Workforce (Employee) Training and Education**

The Privacy Rule requires that covered entities such as UCLA Health System train their Workforce on privacy policies and procedures at a level appropriate for the Workforce members to carry out their roles and responsibilities. All members of the UCLA Health System Workforce will be provided with training on the HIPAA Privacy and Security Rules consistent with their job responsibilities. (*See*: HS Policy No. 9460, "*Privacy and Information Security Workforce Training.*")

XVI. **Unauthorized Release and Disclosure**

The unauthorized release of medical information (including PHI) is a violation of law. Both federal and state laws governing the release of medical record information impose civil and/or criminal liability (including fines) for the inappropriate release of such confidential information. In addition, Workforce members who are found to have violated law and/or UCLA Health System policy may be subject to disciplinary action, up to and including termination. Workforce members should immediately report any unauthorized release or disclosure of PHI to the Office of Compliance Services - Privacy and Information Security and their supervisor (see: HS Policy 9459*,"Privacy and Security Incident Reporting"* and HS Policy No. 9461*, "Privacy and Information Security Sanction"*).

XVII. **Questions Regarding the Release and Disclosure of PHI**

A Workforce member who is uncertain about the appropriate response to a request for PHI should consult his/her supervisor before the information is released. The supervisor should refer any questions regarding the requested release to the Office of Compliance Services - Privacy or the HIMS Department.

In addition, Workforce members need to be aware of and responsive to time constraints in responding to subpoena or other legal requests for disclosure. (*See*: HS Policy No. 9011, *"Legal Processes – Subpoenas, Summons and Complaints.")*

XVIII. **Enforcement**

Failure to follow any provisions of this policy may result in disciplinary action, up to and including termination (*see*: HS Policy No. 9461*, "Privacy and Information Security Sanction.*")

XIX. **Policy Exceptions**

Unless an exception process is specified elsewhere in this policy, 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. The exception request form can be found at http://compliance.uclahealth.org/workfiles/PDF2/HIPAA%20Privacy/HIPAA%20Forms/General%20Exception%20Request%20form.pdf

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
California Lanterman-Petris Short Act ("LPS Act"),
University of California – HIPAA Uses and Disclosures Policy

CONTACT

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

REVISION HISTORY

Approved:	April 8, 2003
Effective Date:	April 14, 2003
Review Date:	July 25, 2012, September 27, 2017
Revised Date:	March 2008, March 31, 2011, August 31, 2012, September 21, 2017

APPROVAL

Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010, 06/27/2012

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

[1.] The Privacy Rule establishes a minimum federal standard for patient privacy. Previously, patient privacy was a matter left up to each state. California, unlike many other states, has had comprehensive patient privacy laws in place for many years. Providers must now conform to both federal and state law, and must comply with whatever provision of the law (California or the Privacy Rule) that is stricter.

Attachments:

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval	Laurie Casaus: Hs Assoc Clin Prof-Hcomp [JM]	9/29/2017
Administration Approval	Roger Lee: Hs Clin Prof-Hcomp [MA]	9/21/2017
Administration Approval	Christopher Tarnay: Hs Assoc Clin Prof-Hcomp [MA]	9/21/2017
Administration Approval	Johnese Spisso: Ceo Med Ctr [MA]	9/21/2017

Step Description	Approver	Date
Executive Medical Boards - MSEC, RNPH PSEC, SMEMB	James Morva: Admin Anl Prn 1	9/21/2017
Hospital System Policy Committee Chair	Margaret Armbruster: Dir [JM]	9/18/2017
Hospital System Policy Committee	James Morva: Admin Anl Prn 1	9/18/2017
	Chloe Ghoogassian: Spec	9/5/2017