



Effective Date: 04/2003  
 Approved Date: 01/2018  
 Revised Date: 01/2018  
 Next Review: 01/2021  
 Owner: Elizabeth Ruszczyk: Dir  
 Policy Area: Compliance  
 Reference Tags: Lippincott  
 Applicability: Ronald Reagan, Resnick, Santa Monica, Ambulatory Care

## Workforce (Including Employee) Access to and Use of Protected Health Information (PHI), HS 9421

### PURPOSE

The purpose of this policy is to provide guidance regarding the access to, and use by, members of the UCLA Health Workforce to Protected Health Information (PHI). When accessing, using or disclosing PHI or when requesting PHI from another covered entity, the UCLA Health Workforce shall make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

### 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").

### POLICY

PHI is confidential and shall not be accessed or viewed other than for the sole purpose of performing employment duties and responsibilities, and applies to oral, written and electronic formats. The extent to which PHI is required to perform job duties varies with the role and function of the Workforce member and unit.

### PROCEDURE

#### I. Workforce Access to Patient Information – "Minimum Necessary"

Access by members of the Workforce to PHI shall be the Minimum Necessary in order to fulfill their assigned responsibilities. (The "Minimum Necessary" standard described in this policy is similar to the University's existing policies that discuss "need to know").

For most job types, the Minimum Necessary requirement will be implemented through education of the individual Workforce member. For certain job types, access restrictions to certain portions of the information systems may also be used. The Minimum Necessary amount of information applies both to

electronic and paper formats of the patient's health information.

**A. Workforce member access to PHI**

- i. UCLA Health Department Managers, or their designee(s), will identify which persons or classes of persons need **access** to PHI to carry out their job duties. For example, nurses, physicians, billers, coders and admissions staff all need access to PHI, but in varying degrees.
- ii. In each area, Departmental Managers or their designee will identify the **types** of PHI to which Workforce members require access. For example, it may be appropriate for physicians to have access to the entire medical record, but scheduling staff only need access to the scheduling applications, and only some security staff may need access to the patient census.
- iii. When possible, applications that provide access to PHI will use role-based access/definitions to restrict user access to the minimum necessary information needed to perform their jobs.
- iv. Reasonable efforts will be made to limit the Workforce's access to PHI to that which is needed to carry out duties.
- v. Managers and supervisors will educate Workforce members on what type and extent of PHI they should access for their job functions. Even when it is not possible to restrict access to the minimum necessary, Workforce members should understand what minimum necessary means in terms of their jobs.

**B. Confidentiality Statement**

On hire, in addition to completing Privacy and Information Security training, each new Workforce member will sign a Confidentiality Agreement (see: Forms Portal form #10342, "*Confidentiality Agreement*") to acknowledge his or her responsibility to protect the confidentiality of patient information and to use only the Minimum Necessary amount of information to accomplish his or her responsibilities.

**C. Unauthorized Use or Disclosure**

The viewing or disclosure of PHI not needed by a Workforce member to carry out his or her job duties constitutes an unauthorized disclosure of that information. Departmental Managers are responsible for monitoring Workforce member activity and imposing discipline in matters of privacy and information security violations.

- i. Workforce members may not access the medical information of family members, co-workers, friends or other individuals for personal or other non-work related purposes, even if written authorization or oral permission has been obtained.

Workforce members designated as "Personal Representatives" should contact the physician or submit a formal request to Health Information Management Services to access the medical information of people for whom they serve as the personal representative. Workforce members must not use their ability to access PHI to obtain medical information for anyone else.

- ii. In those very rare circumstances where a Workforce member's job requires him/her to access and/or copy the medical information of family members, a co-worker, or other personally known individuals, then he/she may do so only to the extent necessary to perform his/her job. However, Workforce members should report the situation to their supervisor who will determine whether to assign a different Workforce member to complete the task involving the specific patient. The Workforce member should continue his/her responsibilities to the extent patient

privacy is not compromised. Information obtained about someone personally known to the Workforce member as part of the Workforce member's job duties should remain confidential and should only be shared with others who have a need to know.

- iii. Workforce members with any concerns on whether their access to PHI is appropriate should ask their supervisors or contact the Office of Compliance Services - Privacy.
- iv. Any unauthorized disclosure of PHI should be reported immediately to the Office of Compliance Services - Privacy and Information Security (see: HS Policy No. 9459, "*Privacy and Security Incident Reporting*").

#### D. Access approval

Access to PHI is approved by Departmental Managers who authorize for each category of job functions those elements of patient information that are generally required to perform the specified job functions. Typically, groups of Workforce members (e.g. grouped by department classification or job function) will have the same access needs. Only the minimum necessary level of access should be granted.

Specifically, for access to ISS-controlled applications, the Departmental Authorizer must verify that such request(s) are appropriate for the job category of the individual for whom the access is requested (see: HS Policy No. 9452, "*User Accounts*").

## II. Exceptions to the Minimum Necessary Standard

The Minimum Necessary requirement does not apply to:

- A. Disclosures to, or requests by, a health care provider for treatment purposes;
- B. Uses or disclosures made to the individual patient or patient's personal representative, as permitted or required;
- C. Disclosures made to the Department of Health and Human Services for compliance or investigation purposes;
- D. Uses or disclosures made pursuant to a valid patient authorization (see: HS Policy No. 9412, "*Authorization to Disclose Protected Health Information*");
- E. Uses or disclosures required for compliance with the standardized Privacy Rule transactions; or
- F. Other uses or disclosures that are required by law (e.g., where a state or other law requires disclosure pursuant to subpoena or court order, for worker's compensation purposes or any other use or disclosure of PHI that is enforceable in a court of law).

## III. Information Needed for Care of Patients

Physicians, nurses, housestaff, and other care providers and students involved in the direct delivery of care may access and use all needed information regarding those patients under their care. ***The entire medical record may be used for patient care purposes*** so that the patient has access to treatment protocols that provide for quality of care, and providers can comply with all state and other laws regarding appropriate and timely treatment.

## IV. Routine and Non-Routine Disclosures

### A. Routine Disclosures

For any type of disclosure that is made on a routine and recurring basis, the PHI disclosed must be limited to the amount reasonably necessary to achieve the purposes of this disclosure.

For routine disclosures to obtain payment, the Minimum Necessary amount of information will be disclosed in accordance with the Privacy Rule payment transaction standards.

**B. Non-routine disclosures**

All non-routine requests shall be forwarded to the departmental supervisor and/or manager, and evaluated on an individual case-by-case basis in accordance with the following criteria to determine what is minimally necessary to accomplish the intended purpose of the disclosure:

- i. Determine the purpose of the disclosure (i.e. treatment, payment, healthcare operations, research, etc.);
- ii. Determine the data needed to support the disclosure; and
- iii. Release or provide access to only the data as determined in the step above.

**C. Judgment of Requesting Party.**

- i. The judgment of the party requesting the information as to the minimum amount of information needed may be relied on if the request is made by:
  - a. A public official or agency for a disclosure permitted;
  - b. Another covered entity;
  - c. A professional who is a Workforce member or business associate; or
  - d. A researcher with appropriate documentation from the IRB.
- ii. UCLA Health System retains the right to make its own Minimum Necessary determinations for disclosures to which the Minimum Necessary standard applies.

In the event a disagreement arises between the requestor and the designated data steward responsible for providing access to the information, the issue will be referred to the Chief Privacy Officer for resolution.

**V. Requesting Protected Health Information from Other Covered Entities**

- A. When requesting PHI from another covered entity (e.g., another physician, hospital, health plan, etc.), UCLA Health System's requests for PHI should be limited to that which is reasonably necessary to accomplish the purpose for which the request is made.
- B. Departmental Managers will review the requests to determine that the PHI sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made. The Office of Compliance Services - Privacy should be consulted if there are any questions.
- C. The entire medical record should not be used, disclosed, or requested except when the entire medical record is specifically justified as the amount of information that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

**VI. Monitoring and Audit**

Review of audit trails and other methods will be used to monitor compliance with this policy.

**VII. Enforcement**

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

**VIII. 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.

#### IX. Questions

Any questions on the Minimum Necessary use or disclosure of PHI should be addressed to the Office of Compliance Services - Privacy and Information Security ([PrivacyInfoSec@mednet.ucla.edu](mailto:PrivacyInfoSec@mednet.ucla.edu)). Also see HS Policy No. 9401, "Protection of Protected Health Information."

## 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, §§1798.29 and 1798.82  
California Health and Safety Code, §§1280.15

## CONTACT

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

## REVISION HISTORY (PRE-POLICYSTAT)

Approved:	April 8, 2003
Effective Date:	April 14, 2003
Review Date:	July 25, 2012, November 15, 2017
Revised Date:	January 23, 2008, March 31, 2011, August 31, 2012, December 29, 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

All revision dates:

01/2018, 08/2012, 03/2011, 01/2008

## Attachments

[2017\\_Privacy Definitions.docx](#)

## Approval Signatures

Step Description	Approver	Date
Administration Approval	Laurie Casaus: Hs Assoc Clin Prof-Hcomp [JM]	01/2018
Administration Approval	Roger Lee: Hs Clin Prof-Hcomp [JM]	01/2018
Administration Approval	Christopher Tarnay: Hs Assoc Clin Prof-Hcomp [JM]	01/2018
Administration Approval	Johnese Spisso: Ceo Med Ctr [JM]	01/2018
Executive Medical Boards - MSEC, RNPH PSEC, SMEMB	James Morva: Admin Anl Prn 1	01/2018
Hospital System Policy Committee Chair	M. Lynn Willis: Mgr	11/2017
Hospital System Policy Committee	James Morva: Admin Anl Prn 1	11/2017
	Nancy Vasto: None	11/2017

COPY