Current Status: *Active* **PolicyStat ID:** *8348223*

Effective Date:	*02/2006*
Approved Date:	*10/2020*
Revised Date:	*10/2020*
Next Review:	*10/2023*
Owner:	*Liangzhou Chen: Mgr*
Policy Area:	*Compliance*
Reference Tags:	*Lippincott*
Applicability:	*Ronald Reagan, Resnick, Santa Monica, Ambulatory Care*

Requests to Interface or Download Restricted Information Policy, HS 9454

PURPOSE

UCLA Health Sciences is responsible for ensuring that Restricted Information (RI) provided via Downloads and/or Interfaces (see definitions in Appendix I) includes the minimum necessary RI, is provided only to those who have a business-related need for the RI, and is protected with appropriate security safeguards.

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 Orthopedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics, the David Geffen School of Medicine, UCLA School of Nursing, UCLA School of Dentistry, and UCLA Fielding School of Public Health (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.

DEFINITIONS

"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:

1. 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.

A. social security number,

B. driver's license number or California identification card number,

C. 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,

D. medical information,

E. health insurance information; or

F. information or data collected through the use or operation of an automated license plate recognition system as defined in California Civil Code §1798.90.5; or

2. 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.

"Minimum Necessary" means reasonable efforts must be made to limit the disclosure to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

"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" 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.

"Workforce" means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Health Sciences, is under the direct control of UCLA Health Sciences or the Regents of the University of California, whether or not UCLA Health Sciences pays them. The Workforce includes employees, faculty, 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 Sciences facilities from another institution.

"Local Manager" – A member of the management team for the requesting business unit, at the director or CAO level, who is authorized to assume liability on behalf of that business unit.

"Data Source" means a database, registry, repository or other data collection whether maintained by ISS or other groups. Some examples of data sources are CareConnect, ISS data marts/constructs, PACS, PODS, Transplant Database, Cancer Registry, and i2b2.

"Download" means a data extract which can be generated manually or by a script and can be in a wide variety of formats including, but not limited to, Excel, text and .xml. Downloads include data provided via extracts by data owners and also via self-service applications such as Tableau.

"Interface" means a method for transmitting data between data sources or between data sources and applications, including, but not limited to HL7, FHIR, DICOM, web services, application program interfaces (APIs), direct messaging, and database connections.

POLICY

Office of Compliance Services (OCS) approval, or that of its delegated Honest Data Brokers, must be obtained in advance for all Interfaces and Downloads of RI with the exception that local managers may approve Downloads for some internal purposes as described in Section VI.

I. **Intended audience**
   This policy will be the most relevant for data source owners, application developers, report developers who provide RI; researchers who wish to obtain RI; and managers who approve requests; not end users who are delivered reports and data by others for internal non-research purposes.

II. **Only the minimum necessary amount of RI should be included in any Download or Interface.**
   When possible, avoid including names, Social Security numbers, healthcare beneficiary IDs, and contact information.

III. **Only provide RI from Downloads and Interfaces to those who have a work-related need for the RI.**

IV. **OCS approval is required in advance for any Interface that will provide access to RI.**

V. **OCS approval is required in advance for Downloads of RI that involve scenarios including those listed below with the exception that local managers may approve Downloads for some internal purposes as described in Section VI.**

   A. Research.

   B. Export to external parties.

   C. Export to UCLA Campus parties who are not also part of UCLA Health Sciences.

   D. Information that is high risk for identity theft or may have additional regulatory requirements for protection, including, but not limited to: Social Security numbers; Healthcare Beneficiary ID numbers; mental health, HIV/AIDS, and substance abuse information.

   E. Sensitive information that has regulatory or contractual requirements for limited access or data security. Examples of sensitive information would be data provided by external parties such as Accountable Care Organizations, business partners, California's Office of Statewide Health Planning and Development (OSPHD), etc., as well as research and industry data registries/repositories where data use or other agreements may include specific data security requirements.

   F. Fund raising or marketing.

   G. CareConnect Reporting Workbench export privileges.

VI. **Local managers may approve Downloads of RI for internal purposes if all the conditions below are met**:

   A. No research, fund raising or marketing, interfaces, or exports to external parties is involved.

   B. The Downloads will only be used by internal customers of the group that provides the report/data extract. For example, departmental developers and report writers may provide data extracts and reports containing RI to their own internal customers. Teams such as Decision Support that provide reporting for Enterprise-wide operations may provide data extracts and reports containing RI to their customers.

   C. No individually identifiable mental health information may be shared outside of the department where the individuals were encountered except for payment purposes.

D. No individually identifiable information about sensitive diagnoses or situations is involved, including but not limited to: HIV/AIDS, abortion, adult and child abuse, the pregnancy of a minor, substance abuse, rape/sexual assault, and sexually transmitted diseases (STDs). The regulations around the use and disclosure of this kind of information are complicated, so OCS should always be consulted.

VII. **How to submit a Request to Download/Interface Restricted Information**

A. For requests for Downloads of clinical information for research, please follow the UCLA Clinical and Translational Science Institute (CTSI) process for Clinical Data Requests.

B. For all other Interface or Download requests, please either fill out the online version of the Request to Interface/Download form available through Collibra or download the **OCS Request to Interface/ Download form**, complete it and email it back to CompOffice@mednet.ucla.edu.

C. The Chief Administrative Officer (or designee) of the requester's department must sign the form to accept the responsibility that the department may be held responsible for the notification costs of any breaches of Restricted Information that will be obtained via the Download/Interface.

D. See **Appendix 2 - Information for Requests** for details on the types of information that will be collected for requests.

VIII. **OCS Review and Approval**

OCS or designee will review the request, taking into consideration the issues documented in **Appendix 3 - OCS Review,** and will follow up with the requester for additional information as necessary. If denied, OCS will respond to requester. If approved, OCS will sign or otherwise indicate approval and return the final version of the form to the requester.

IX. **Data Security; System and Audit Trails; Random Security Audits**

All systems which are used to store and access RI must meet the requirements specified in HS Policy No. 9457, *"**Minimum Security Standards**"* and its associated Standards.

X. Systems (other than individual workstations) which are used to store and access RI must have logging capabilities which meet the requirements described in HS Policy No. 9462, *"**Privacy and Information Security Monitoring and Auditing**"* and its associated Standard.

Random audits may be performed by OCS - Privacy and Security and/or designees to ensure the adequacy of the security protections on the systems and data, and to ensure that the access to the data is in compliance with HS Policy No. 9401, *"**Protection of Confidential Patient Information (Protected Health Information (PHI))**,"* and HS Policy No. 9421, *"**Workforce (Including Employee) Access to and Use of Protected Health Information (PHI)**."*

XI. **Breaches of Patient Privacy or Data Security**

In the event a violation of patient privacy or system or data security breach occurs, the person or department identifying the breach must contact the Office of Compliance Services - Privacy and Information Security (CompOffice@mednet.ucla.edu, (310)794-6763) immediately. The Chief Privacy Officer and/or Chief Compliance Security Officer will investigate the breach in accordance with HS Policy No. 9459, *"Privacy and Information Security Incident Reporting,"* and corrective action may be taken in accordance with HS Policy No. 9490, *"Mitigation,"* and HS Policy No. 9461, *"Privacy and Information Security Sanction Policy."*

XII. **Questions**

Any questions about Downloading or Interfacing to Restricted Information should be referred to the Office of Compliance Services - Privacy and Information Security (CompOffice@mednet.ucla.edu).

XIII. **Enforcement**

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

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164

Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2

California Lanterman-Petris-Short Act ("LPS Act")

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 1280.18

University of California Business and Finance Bulletin IS-3, Electronic Information Security

University of California Electronic Communications Policy (ECP)

CONTACT

Chief Privacy Officer, Office of Compliance Services

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY (PRE-POLICYSTAT)

Approved:	February 22, 2006
Effective Date:	April 20, 2005, July 26, 2017
Revised Date:	November 2005; June 21, 2007; May 30, 2008, March 31, 2011, August 31, 2017

APPENDIX 2 - INFORMATION FOR REQUESTS

1. **Information that should be provided for Requests to Interface or Download**

   A. The name of the person or department requesting the Download/Interface who will be responsible for safeguarding the Restricted Information (RI)

   B. The name of the Chief Administrative Officer (or designee) who will accept the liability for notification costs should there be any breach of the RI requiring notification.

   C. A description of the project or purpose for which the RI will be provided.

   D. What data are needed?

      i. The selection criteria for the data. Rarely is data for all patients necessary, so a list of inclusion/exclusion criteria is important. This includes whether Mental Health, Substance Abuse, or HIV/AIDS information will be involved

      ii. A list of data elements being requested.

      iii. The frequency for providing RI, including end dates if applicable

      iv. The number of records being requested.

E. How the data will be accessed/transmitted/maintained.

i. Which group(s) will have access to the RI?

ii. How the RI will be transferred securely.

iii. Where the RI will be stored.

iv. A description as to whether the RI will be re-disclosed to others, including any potential external disclosures.

v. The plan for return or destruction of the RI when the purpose is completed, if applicable.

F. If data will be maintained anywhere except on an ISS or departmental file share, an ISS/DGIT controlled environment or UCLA Health Box, a risk assessment may be required.

G. If the request is for research, copies of the IRB approval, the IRB application, the Informed Consent forms, and any relevant protocols.

H. If the data are being requested for internal research purposes, then the request must include a valid signed Internal Data Use Agreement (DUA).

I. Copies of any relevant Agreements including, but not limited to, Purchasing Agreements, Data Use Agreements, Purchasing Agreements, external Data Security Requirements, Participation Agreements, and/or HIPAA Business Associate Agreements.

APPENDIX 3 - OCS REVIEW

1. **Privacy Review**
   The Chief Privacy Officer or designee will review the request including, but not limited to, consideration of the issues below:

A. The information requested is a permitted disclosure for the purpose identified in the request, and that any applicable patient authorizations have been obtained.

B. The amount of information requested complies with the minimum necessary amount of information for the purpose of HS Policy No. 9421, *"**Workforce (Including Employee) Access to and Use of Protected Health Information**."*

C. If the disclosure is an accountable disclosure, a process has been established to provide an upload or tracking record to the UCLA Health System PHI Tracking System.

D. For disclosures requiring a Data Use Agreement or Business Associate Amendment, the documents have been obtained and meet UCLA requirements.

E. Assessment that any legal issues and risk to UCLA Health Sciences raised by the use and/or disclosure have been identified and the use of the information provides a minimal risk to patient privacy.

F. The plan for the protection of the information and the disposal of identifiers, if applicable, meets standards.

2. **Information Security Review**
   The Chief Compliance Security Officer or designee will review the request, including, but not limited to, consideration of the issues below:

A. Any external data security requirements included in the HIPAA Business Associate Agreement, Data Use Agreements or other Agreements can be met.

B. System security protections meet all UCLA Health security requirements including, but not limited to:

  i. Acceptable risk assessment results
  ii. Secure transmission of data, if applicable from the receiving system to other systems and/or devices
  iii. Appropriate access controls, such as password and authentication of user
  iv. Audit trails are maintained with required data elements such as timestamp, user id, user name, patient name, MRN, activity description, computer name, IP address, etc.
  v. Secure system configurations
  vi. Disaster recovery and backup plans
  vii. Physical security of system(s) and data
  viii. Procedures for termination of access

All revision dates:	10/2020, 08/2017, 03/2011, 05/2008, 06/2007, 11/2005

Attachments

No Attachments

Approval Signatures

Step Description	**Approver**	**Date**
Administration Approval- President and CEO, UCLA Health	Johnese Spisso: Ceo Med Ctr [JB]	10/2020
Ronald Reagan Medical Staff Executive Committee- Chief of Staff	Carlos Lerner: Assoc Prof Of Clin-Hcomp [JB]	10/2020
Santa Monica Medical Staff Executive Committee- Chief of Staff	Roger Lee: Hs Clin Prof-Hcomp [JB]	10/2020
Resnick Neuropsychiatric Medical Staff Executive Committee- Chief of Staff	Aaron Kaufman: Hs Assoc Clin Prof-Hcomp [JB]	10/2020
Hospital System Policy Committee Chair	Jeffrey Bergen: Mgr [KK]	08/2020
Policy Owner	Liangzhou Chen: Mgr	08/2020