CURRENT STATUS: Active

Effective Date: 2/22/2006
Review Date: 8/31/2017
Revised Date: 8/31/2017
Next Review: 8/30/2020

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

Requests to Interface or Download Restricted Information Policy, HS 9454

PURPOSE

UCLA Health Sciences is responsible to ensure 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 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.

POLICY

Office of Compliance Services (OCS) approval must be obtained in advance for all Interfaces and Downloads 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 ID 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 any of the issues below with the exception that local managers may approve Downloads for some internal purposes as described in Section VI.

1. Research
2. Export to external parties
3. 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 and substance abuse information
4. 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.
5. Fund raising or marketing
6. CareConnect Reporting Workbench export privileges

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

1. No research, fund raising or marketing or exports to external parties is involved.
2. 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.
3. No individually identifiable mental health information may be shared outside of the department where the individuals were encountered except for payment purposes.
4. No individually identifiable substance abuse information is involved. The regulations are complicated so OCS should always be consulted for reports and extracts involving substance abuse information.

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

1. For requests for Downloads of clinical information for research, please follow the UCLA Clinical and Translational Science Institute (CTSI) process for Clinical Data Requests.
2. For all other Interface or Download requests, please download the OCS Request to Interface/Download form, complete it and email it back to InfoSecAll@mednet.ucla.edu.
3. 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.
4. 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
IX. Random Security Audits; System and Audit Trails
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 and Use of PHI," and HS Policy No. 9421, "Workforce Access to and Use of PHI."

X. 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 (PrivacyInfoSec@mednet.ucla.edu, 310 794-8638) 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."

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

XII. 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 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, Office of Compliance Services
Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

<table>
<thead>
<tr>
<th>Approved:</th>
<th>February 22, 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>April 20, 2005, July 26, 2017</td>
</tr>
</tbody>
</table>

APPROVAL
Johnese Spisso, RN, MPA
President UCLA Health
APPENDIX 1 - 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.

"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.

“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.

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 with 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.

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 is needed and how it will be accessed/transmitted/maintained
   a. A list of data elements and selection criteria, including if Mental Health or Substance Abuse information will be involved
   b. The frequency for providing RI, including end dates, if applicable
   c. Who will have access to the RI
   d. How the RI will be transferred securely
   e. Where the RI will be stored
   f. A description as to whether the RI will be re-disclosed to others, including any potential external disclosures
   g. The plan for return or destruction of the RI when the purpose is completed, if applicable

E. A copy of the most recent risk assessment for all systems involved
F. If the request is for research, copies of the IRB approval, the IRB application, the Informed Consent and any relevant protocols.

G. If a Limited Data Set is being requested (as defined in HS Policy No. 9440, "Release of Protected Health Information for Research"), then the request must include a valid signed Data Use Agreement.

H. Copies of any relevant Agreements including, but not limited to, Purchasing Agreements, Data Use Agreements, Purchasing Agreements, external Data Security Requirements, Participation Agreements, 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 Access to/Use of Protected Health Information (Minimum Necessary Standard)."

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:

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

2. System security protections meet all UCLA Health security requirements including, but not limited to:
   i. Acceptable risk assessment results
   ii. Appropriate access controls, such as password and authentication of user
   iii. Audit trails are maintained with required data elements such as timestamp, userid, user name, patient name, MRN, activity description, computer name, IP address, etc.
   iv. Secure system configurations
   v. Disaster recovery and backup plans
   vi. Physical security of system(s) and data
vii. Procedures for termination of access
viii. Secure transmission of data, if applicable from the receiving system to other systems and/or devices

Attachments:
No Attachments

Approval Signatures

<table>
<thead>
<tr>
<th>Step Description</th>
<th>Approver</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Approval</td>
<td>Laurie Casaus: Hs Assoc Clin Prof-Hcomp [JM]</td>
<td>8/31/2017</td>
</tr>
<tr>
<td>Administration Approval</td>
<td>Roger Lee: Hs Clin Prof-Hcomp [MA]</td>
<td>8/31/2017</td>
</tr>
<tr>
<td>Administration Approval</td>
<td>Christopher Tarnay: Hs Assoc Clin Prof-Hcomp [MA]</td>
<td>8/31/2017</td>
</tr>
<tr>
<td>Administration Approval</td>
<td>Johnese Spisso: Ceo Med Ctr [MA]</td>
<td>8/31/2017</td>
</tr>
<tr>
<td>Executive Medical Boards - MSEC, RNPH PSEC, SMEMB</td>
<td>James Morva: Admin Anl Prm 1</td>
<td>8/31/2017</td>
</tr>
<tr>
<td>Hospital System Policy Committee Chair</td>
<td>Margaret Armbruster: Dir</td>
<td>7/27/2017</td>
</tr>
<tr>
<td>Hospital System Policy Committee</td>
<td>James Morva: Admin Anl Prm 1</td>
<td>7/26/2017</td>
</tr>
<tr>
<td></td>
<td>Ann Chang: Dir</td>
<td>7/20/2017</td>
</tr>
</tbody>
</table>