UCLA Health System

REQUEST TO INTERFACE OR DOWNLOAD RESTRICTED INFORMATION

Request Number (assigned by Compliance):	
NAME OF PERSON COMPLETING THE REQUEST:	
REQUESTING DEPARTMENT/DIVISION:	Date of Request:

DATA SCOPE: ☐ UCLA Medical Center ☐ UCLA Santa Monica ☐ NPH
☐ Outpatient Hospital ☐ Outpatient non-hospital ☐ Inpatient data ☐ CPN
☐ Practice Group ☐ Other: _____

General Category: ☐ Treatment (Patient Care) ☐ Payment ☐ Operations
☐ Government or other mandatory reporting
☐ Research – Please complete Research section on next page
☐ Other (specify):

PURPOSE (*Provide description)*

Data Source: ☐ CareConnect ☐ xDR ☐ ESPI ☐ PODS ☐ Signature
☐ Lab Results ☐ PACS ☐ PowerPath
☐ Other (specify):

Data Type:

☐ Documents	☐ Laboratory Results	☐ Diagnostic and Procedure coded data
☐ Patient identification data (specify)		
☐ Digital Images (specify)	☐ Film/video	☐ Charge and/or Billing Data

List all data elements (or attach list). Include any selection criteria.

Download Method: __ HL7 interface __ Data extract __ DICOM __ Web Services
___ Other (specify) _____
Frequency of Download: _____ (e.g. one-time, monthly, quarterly, annually)
Volume of Data: _____ (number of patients/records)
Date Range: From _____ to _____

UCLA Health System

Data will be held by:

- ☐ Requesting department/user
- ☐ Other recipient within Mednet (specify):
- ☐ UCLA Recipient outside Mednet (specify):
- ☐ External vendor (specify):
  For vendors, is a fully-executed BAA in place?: ☐ Yes ☐ No
- ☐ Other external recipient (specify):

Data Transmission:

- ☐ Data will be transferred within Mednet using:
  - ☐ Mednet email ☐ Mednet fileshare ☐ Webservices, FTP, HL7 within Mednet
  - ☐ DICOM ☐ Other internal delivery (specify):

- ☐ Data will be transferred to locations external to Mednet using:
  - ☐ Mednet Business-to-Business VPN ☐ Mednet Software Client VPN
  - ☐ Other email (specify):
  - ☐ Other (specify):

Data will be maintained:	Estimate of time frame data will be maintained:
☐ In application ☐ In database	☐ Permanently
☐ On MITS or departmental file share	☐ Data will be returned or destroyed after use (explain):
☐ On user workstation	
☐ Other (specify):	☐ Other (explain):

DATA SECURITY ASSESSMENT

If data will be maintained anywhere except on a MITS or departmental file share:

- ☐ Attach COMPLETED OR UPDATED InfoSec Review Form for electronic system in which data will be stored, maintained and/or transmitted

Research Request Details (only complete this section if the download request is for research)

All requests for PHI for Research Purposes must be approved by the UCLA IRB and documentation attached. Request will not be considered without this information.

Authorization for Disclosure

- ☐ IRB Waiver of Authorization (attached)
- ☐ Individual Patient Authorizations (attached)
- ☐ De-identified Data only
- ☐ Limited Data Set (Data Use Agreement Attached)

Other IRB documentation

- ☐ IRB Approval (attached)
  IRB #: Study Start Date: Study End Date:
- ☐ IRB Application (attached)
- ☐ IRB Application - Data Security Plan (attached)
- ☐ IRB Application - List of Data Elements (attached)

UCLA Health System

Research Data to be accessed by or shared with:

☐ Research Staff only ☐ Researchers at other sites (specify)_____

☐ Research sponsor_____

☐ Government entity (e. g. FDA, NIH, etc)

Requesting Department Signature and Acknowledgement:

I understand that if UCLA Health determines that UCLA is required to notify patients or other individuals regarding any breaches of unencrypted Restricted Information (see reverse for definitions) that may arise from this requested access, my department can be held fully responsible for any and all notification costs

_____ _____

Name Signature Date

_____ _____

CAO or Designee Signature Date

☐ Additional information needed to approve request:

PRIVACY OFFICER (or designee):

☐ Approved as identified above

☐ Approved with following limitations/enhancements:

☐ Not Approved due to:

_____ _____

Name: Signature Date

SECURITY OFFICER (or designee):

☐ Approved as identified above

☐ Approved with following limitations/enhancements:

☐ Not Approved due to:

_____ _____

Name: Signature Date

Reference: HS Policy No. 9454, "*Requests to Interface or Download Restricted Information*"

UCLA Health System

Definitions:

"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 below but could also include other types of information such as intellectual property, proprietary information, research protocols, research results, student information, animal research information, passwords, and other confidential information that could damage the reputation of the institution.

"Protected health information" or "PHI" is any individually identifiable health information, in any format, including verbal communications, regarding a patient created as a consequence of the provision of health care. "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.

Below are listed the 18 identifiers that must be removed to consider data de-identified according to the HIPAA Privacy Rule. Note it only takes one identifier for data to be considered as containing PHI.

- Name (includes initials)
- Street Address, City, State and Zip code
- Dates (birth, death, treatment, etc.)
- Phone
- FAX
- Email
- SSN
- Med. Rec. #
- Account #
- Health Plan Beneficiary #
- Certificate License #
- Vehicle ID (VIN) & Drivers License ID
- Device ID or Serial #
- Web URL
- IP Address
- Biometric IDs, including finger- or voice-prints
- Full-face photos or comparable images
- Any other unique ID #, characteristic or code.

"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)*" 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.