

# Request for Access to Sensitive Data

Revision A

Dean's Office  
Information Services Unit  
Issue Date: 1/4/2005  
Last Revision: 5/17/2005

Please **fax** completed form to the ISU Helpdesk at **415-502-2255**  
This document cannot be processed until it is **COMPLETELY** filled out  
For assistance, please call the ISU Helpdesk at 415-502-1919

## SECTION 1: REQUEST TYPE

New Request       Add or Change to existing User Account. Provide login ID: \_\_\_\_\_

## SECTION 2: SUBMITTER AND USER IDENTIFICATION

Submitted by: \_\_\_\_\_  
Last Name                      First Name                      Phone

Requested for: \_\_\_\_\_  
(User)                      Last Name                      First Name                      Phone

Employee     Temporary     Consultant

Department: \_\_\_\_\_

## SECTION 3: DESCRIBE SENSITIVE DATA (see Definitions section next page)

Personal/Confidential     Financial     HIPAA (ePHI)     SB1386

Briefly describe data content, e.g., SSN, Home Address, Medical Record Number, etc.

Identify and describe source(s) of data, e.g., e-mail, Oracle ad-hoc personnel database, desktop, shared files, etc.

Briefly describe business need/purpose and under what circumstances must the data be accessed

## SECTION 4: SIGNATURES

Department Manager Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_ Phone: \_\_\_\_\_

User Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Data Owner Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_ Phone: \_\_\_\_\_

(Data Owner may not apply: call ISU)

**For ISU Use Only:** Tech Name: \_\_\_\_\_ Request Implemented?  Yes  No Date: \_\_\_\_\_

## 1. Purpose

This form is required as a record and request for access to sensitive data residing on computer systems supported by the School of Medicine Dean's Office Information Services Unit (ISU).

## 2. Definitions

### 2.1. Access

Access is defined as permission to view, alter, retrieve, transmit, or store sensitive data via electronic devices (computers, servers, etc.), portable media (laptops, CDS, portable hard drives, floppies, etc.), software applications, databases, file transfer protocol (FTP), internet, or e-mail, etc.

### 2.2. Sensitive Data

Sensitive data in regards to this form is defined as confidential, personal, and financial data including all data protected by HIPAA and SB1386.

#### 2.2.1. Confidential and Personal Data

Confidential and personal data includes staff, faculty, student information that resides in local electronic files or in the ad-hoc Campus Personnel and Payroll Oracle databases. Examples of this information include:

<ul style="list-style-type: none"><li>• Academic Evaluations</li><li>• Letters of Recommendation</li><li>• Physical Condition</li><li>• Psychological Condition</li><li>• Performance Evaluations</li><li>• Corrective Actions</li></ul>	<ul style="list-style-type: none"><li>• Current rate of pay</li><li>• Citizenship</li><li>• Social Security Number</li><li>• Home Address</li><li>• Home Telephone Number</li><li>• Income Tax Withholding</li><li>• Spouses or Other Relatives Names</li></ul>
--	---

Derived from UCOP's Legal Requirements on Privacy of and Access to Information  
More Info: <http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html>

#### 2.2.2. Financial Data

Financial data includes any departmental, staff, faculty, or student financial information/transactions that reside in local electronic files or in the ad-hoc Campus Financial Oracle databases. Note, for Weblinks access please contact Alexis Purcell in Dean's Office Finance.

### 2.2.3. HIPAA Data

HIPAA security regulations require that all protected health information (PHI) have adequate security protections and that the university maintain documentation of risk assessment, monitoring, and other security parameters for PHI stored electronically (45 CFR Part 164).

Protected or personal health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

**If any of these data fields are associated with health information then they become PHI:**

<ul style="list-style-type: none"><li>• Names</li><li>• Dates</li><li>• Postal Addresses</li><li>• Phone Numbers</li><li>• Fax Numbers</li><li>• Email addresses</li></ul>	<ul style="list-style-type: none"><li>• Social Security Numbers</li><li>• Medical Record Number</li><li>• Health Plan Number</li><li>• Account Numbers</li><li>• License/Certificate Numbers</li><li>• Vehicle ID Numbers</li></ul>	<ul style="list-style-type: none"><li>• Device Identifiers</li><li>• Web URLs</li><li>• IP Address Numbers</li><li>• Biometric Identifiers</li><li>• Photos/comparable images</li><li>• Any other unique identifier</li></ul>
--	---	---

More Info: <http://www.ucsf.edu/hipaa/>

### 2.2.4. SB1386 Data

UCSF complies with the provisions of California Privacy Legislation, California Senate Bill 1386 (SB1386), requiring notification to California residents regarding any breach to the security of a computing system where there is a reasonable belief that an unauthorized person has acquired their unencrypted personal information.

**SB1386 covers the unauthorized disclosure of any of the following identifiers in combination with an individual's first name or first initial and last name:**

<ul style="list-style-type: none"><li>• Social Security Number</li><li>• Driver license number or California identification card number.</li><li>• 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</li></ul>
--

More Info: <http://isecurity.ucsf.edu/main.jsp?content=compliance/sb1386>