

University of California  
San Francisco

Medical Center



## HEALTH INFORMATION MANAGEMENT SERVICES CLINICAL INFORMATION SERVICES

FOR MORE INFORMATION VISIT OUR WEBSITE AT: <http://hims.ucsfmedicalcenter.org/stor>

### REQUEST FOR AUTHORIZATION TO STOR/CDS

A **Computer Security and Use Statement** is required for all users.

#### NEW USER (NEVER USED STOR)

The entire form(s) must be filled out in order to gain access to STOR/CDS. Forms not thoroughly completed shall be returned to the applicant for completion. Applicants are required to have their supervisor's sign both forms

When both forms have been completed send both forms back to the CIS Input Unit at Campus **Box 0308** or mail it to **HIMS Dept. (STOR), 185 Berry St. St. 2000, S.F. CA, 94143-0308**, or **FAX it to 353-2484**. You will be called soon after to schedule a training session.

Please be prepared for Training and bring your Employee Identification Badge. If you have any questions or concerns please call the **CIS unit at 353-2189**. Thank you.

#### RE-AUTHORIZATION

RECLASSIFICATION

FORGOT PASSWORD

Complete the information below and telephone the CIS unit of Health Information Management Services at 353-2189 to obtain forgotten STOR system Login ID codes or Security Access codes. **You may FAX the information to 353-2484.**

If you are a member of the Inpatient Nursing Staff you should return this completed form to **Nursing Administration** at **FAX 353-8562; VOICEMAIL 353-1810 or 353-1670.**

UCSF computer system users have access to confidential medical information. This information is maintained to serve the patient, health care providers and to conform to regulatory requirements. Patient data is confidential and may not be revealed to unauthorized persons, agencies, etc. without written consent of the patient.

### USE OF ANOTHER PERSON'S ID AND SECURITY ACCESS CODE IS PROHIBITED

LAST NAME \_\_\_\_\_ FIRST NAME \_\_\_\_\_ MIDDLE INITIAL \_\_\_\_\_

UCSF DEPARTMENT \_\_\_\_\_ BOX # \_\_\_\_\_ FAX # \_\_\_\_\_

BUSINESS ADDRESS \_\_\_\_\_ BUSINESS # \_\_\_\_\_

JOB TITLE \_\_\_\_\_ EMPLOYEE ID# \_\_\_\_\_

APPLICANT'S SIGNATURE \_\_\_\_\_ DATE \_\_\_\_\_

JOB STATUS: \_\_\_ Permanent \_\_\_ Per diem \_\_\_ Temp \*\*Expiration date (if temp): \_\_\_\_\_

PLEASE CHECK ONE:  Medical Center  School of Medicine  School of Nursing

#### WHY DO YOU NEED STOR ACCESS?

- UCSF Patient Care Area  
 Research (attach a copy of CHR approval)  
 Billing  
 Other (describe) \_\_\_\_\_

#### User Class:

- M.D.  
 Inpatient Staff (fax: 353-8562)  
 Outpatient Staff  
 Medical Student (fax: 476-0714)

#### Function:

- Patient lookup  
 Print STORsheets  
 Other (describe) \_\_\_\_\_

SUPERVISOR'S NAME \_\_\_\_\_ SUPERVISOR'S PHONE \_\_\_\_\_

SUPERVISOR'S SIGNATURE \_\_\_\_\_ DATE \_\_\_\_\_

(Office use only)

Received ON \_\_\_\_\_ STOR Authorizer \_\_\_\_\_ Authorized Date: \_\_\_\_\_ LOGIN ID: \_\_\_\_\_  
 Security Access Code deleted? \_\_\_ Re-Activation Date: \_\_\_\_\_ Phone Calls (date): \_\_\_\_\_ Appt. (date/time): \_\_\_\_\_



# HEALTH INFORMATION MANAGEMENT SERVICES CLINICAL INFORMATION SERVICES

FOR MORE INFORMATION VISIT OUR WEBSITE AT: <http://hims.ucsfmedicalcenter.org/stor>

## COMPUTER SECURITY AND USE STATEMENT REGARDING ACCESS TO PATIENT INFORMATION IN THE UCSF MEDICAL CENTER SYSTEM

Applicant's Name  \*Employee Number   
 (REQUIRED)

UCSF Department

UCSF faculty and staff employees, house staff, students, contractors may have access to protected health information. This information is maintained to serve the patient, health care providers, third-party payers, health care research and to conform with regulatory requirements.

Patient information is accessible only to authorized personnel. It is your responsibility as an authorized user to preserve and protect the privacy, confidentiality and security of all medical records, proprietary and other confidential information relating to UCSF, its patients, activities and affiliates, in accordance with the law and University policy.

1. Patient data is confidential and may not be revealed to unauthorized persons, agencies, etc., without the written consent of the patient. If there are any questions, please consult a supervisor, manager, chief resident, or attending physician.
2. There will be no discussion of a patient's medical or financial condition with non-authorized personnel.
3. Access to patient data is restricted unless required to fulfill the course of job responsibilities.
4. Under Federal and California state law, any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program or data shall be guilty of a felony and personally liable for damages.
5. The unauthorized use of another person's security code/password, or the unauthorized delegation of my code to another person may be considered false representation.

- I have read the above COMPUTER SECURITY AND USE STATEMENT.
- I understand and agree that in the performance of my duties I must secure and hold a patient's medical and/or financial information in confidence.
- I understand that under provisions of the California CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CIVIL CODE SECTION 56) and/or the Federal HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996, intentional or involuntary violation of confidentiality may result in disciplinary action up to and including dismissal from employment, fines and imprisonment. Violation of Local, State or Federal statutes may carry the additional consequence of prosecution under the law.
- I understand that it is my responsibility to follow safe computing guidelines, including:
  - Protect my User ID(s) and password(s)
  - Use strong passwords; use a password-protected screensaver
  - Always log off shared workstations
- I understand that my User ID(s) constitutes my signature and I will be responsible for all entries made under my User ID(s).

\_\_\_\_\_  
Applicant's Signature Date

\_\_\_\_\_  
Supervisor's Signature Date