



UNIVERSITY of CALIFORNIA, SAN DIEGO  
HEALTH SCIENCES

# *Privacy and Security Training for Health Science Workforce Members*

---

UCSD Health Sciences

April 22, 2009

This training module satisfies Federal laws which mandate workforce privacy / security training at the time of hire and UC policy for annual privacy training for Health Insurance Portability and Accountability Act (HIPAA) and the California Confidentiality of Medical Information Act (CMIA)

# Who must complete privacy / security training at UCSD?

- Anyone who works with or may see health, financial, or confidential information with personal identifiers
- Anyone who uses a computer or electronic device to store and/or transmit personal or health information
- Such as:
  - Medical Center / Medical Group employees
  - Schools of Medicine / Pharmacy employees, health professions trainees
  - Campus administrative & technical staff who work in clinical areas
  - Volunteers (Including Volunteer Clinical Faculty)
  - Students who work in patient care areas
  - Research staff and investigators
  - Accounting, Payroll and Benefits staff
  - Other independent contractors with access to UC's personal / health information who assist UCSD employees with their job

---

# Objectives

- Understand what information must be protected under state and federal privacy laws
  - Understand your role in maintaining privacy and security of protected health information (PHI)
  - Understand what rights patients have regarding access and use of medical information
  - Understand your role with adhering to data security standards and responsibility for reporting incidents
  - Understand the consequences and risks of individual penalties for non-compliance
-

- HIPAA: Health Insurance Portability and Accountability Act of 1996. The purpose of the law was to make health insurance more efficient and portable.
- Because of public concerns about confidentiality, it also addressed information protection.

HIPAA

*Privacy Standards:  
April 2003*

Protect an individual's health information and provide patients with certain rights

*Security Standards:  
Final Rule Published  
February 20, 2003*

Physical, technical and administrative safeguards of patient information that is stored electronically.  
(Effective: **2005**)

*Codes and Transaction  
Standards:  
October 2003*

Standardization for electronic billing and claims management.

---

# Confidentiality of Medical Information Act (CMIA)

- CMIA prohibits disclosure of “medical information” without prior authorization unless permitted by law.
    - (California Civil Code 56.10)
  - ***Medical information*** means any individually identifiable information in the possession of or derived from a provider of health care regarding a patient’s medical history, mental or physical condition, or treatment.
    - (California Civil Code 56.05(g))
-

---

# What information must you protect?

## PHI

- Protected health information (PHI) is any personal or health information UCSD creates or maintains in the course of providing treatment, obtaining payment for services, or while engaged in health care operations including teaching and research activities.
  
- Common examples of PHI include:
  - Medical records, test results and treatment plans
  - Billing records, referral authorizations and health insurance information
  - Name, address, social security number and photographs
    - To view a complete list of 18 PHI identifiers, <http://health.ucsd.edu/compliance/hipaa.shtml>

---

# To the Patient, It's All Confidential Information

- Patient *Personal* Information
- Patient *Financial* Information
- Patient *Medical* Information
- Written, Spoken, Electronic PHI
  
- **Patient Information may be accessed, used or disclosed only to do your job**

---

# Requirements before PHI is Used or Disclosed

- In order for UCSD to use or disclose PHI:
  - The University must give each patient a “Notice of Privacy Practices” that:
    - Describes how the University may use and disclose the patient’s protected health information (PHI) **and**
    - Advises the patient of his/her privacy rights
  - The University must attempt to obtain a patient’s signature acknowledging receipt of the Notice, except in emergency situations. If a signature is not obtained, the University must document the reason.
  - The University must provide privacy / security training to its workforce.

---

# Employee Access to Protected Health Information (PHI)

- Patient information is confidential and shall not be accessed or viewed other than for the sole purpose of performing employment duties and responsibilities
  - **Accessing a record, including your own or that of a family member or friend without a work purpose is a violation of UCSD policy**
  - UCSD monitors electronic access of PHI to assure compliance
  - Inappropriate access to patient information may result in disciplinary action up to and including termination as well as **individual fines.**
-

---

# You may...

- **Look** at a patient's PHI **only** if you need to do so for your job
  - **Use** a patient's PHI **only** if you need to do so for your job
  - **Disclose** a patient's PHI to others **only** when it is necessary for others to do their job
  - **Limit** your access, use and disclosure of PHI to the minimum necessary information needed to perform your job.
-

---

# PHI may be Used and Disclosed for the Following Purposes:

## ■ Treatment:

- We may use and disclose medical information about a patient to health system doctors, nurses, technicians, students or providers who are involved in the patient's care

## ■ Payment:

- We may use and disclose medical information about the patient so that the treatment and services received may be billed and payment may be collected – **subject to the minimum necessary standard**

## ■ Operations:

- We may use and disclose medical information for teaching, medical staff peer review, legal purposes, internal auditing, to conduct customer service surveys, and general business management – **subject to the minimum necessary standard**
-

# Other Permitted Uses and Disclosures

- For appointment reminders
  - Take care to avoid leaving messages on answering machines which disclose sensitive information.
- To provide treatment alternatives
- To provide limited information about patients for the hospital directory
- To assist other individuals involved in the patient's care (e.g., friends, family, etc.), if determined to be in the patient's best interest.
- For disaster relief efforts
- For **research** (with HRPP / IRB approval)
- For **fundraising**, using limited demographic information

---

# Other Permitted Uses and Disclosures

- **To avert serious threat to health and safety**
  - For organ and tissue procurement, reimplantation, or banking purposes
  - To military command authorities about armed forces patients
  - To workers' compensation programs (*minimum necessary*)
  - **For public health disclosures**
  - **For government oversight activities**
  - **To law enforcement, for certain activities**
  - To coroners, medical examiners and funeral directors
  - For national security and intelligence activities
  - To correctional institutions about inmates
  - For certain legal proceedings, lawsuits and other legal activities
  - To business associates with a written business associate agreement
-

---

# Examples of Permitted Uses and Disclosures

- **To avert a serious threat to health or safety:** PHI may be used to prevent or lessen a serious and imminent threat to a person or the public.
- **Public-health disclosures:** PHI may be used to report data to prevent or control disease, injury or disability as required by law (e.g., reporting of disease, injury, vital events such as birth or death).

---

# Continued Examples of Permitted Uses and Disclosures

- **Government health oversight activities:** PHI may be used for government or certification audits: civil, administrative, or criminal investigations or proceedings; or licensure or disciplinary action
  
- **Law enforcement:** PHI may be used to report suspected abuse, neglect or domestic violence; death resulting from criminal conduct; criminal conduct occurring on premises; or limited PHI for identifying or apprehending a suspect, witness or missing person
  
- **Individuals involved in the patient's care or payment of care:** PHI may be disclosed to a family member, relative (or anyone identified by the patient as involved in the patient's medical care or assisting in paying for a patient's medical care), IF...
  - The patient agrees or had an opportunity to object to the disclosure, and did not; or
  - Based on the exercise of professional judgment, it appears that the patient would not object to the disclosure; or
  - In cases where the patient is not present or incapacitated, the disclosure is in the best interests of the patient, based on the exercise of professional judgment.

---

# Continued Examples of Permitted Uses and Disclosures: Marketing

- A UCSD provider may use PHI to communicate to a patient about a product or service that UCSD Medical Center provides.
- A UCSD provider may use PHI to communicate to a patient about general health issues, e.g., disease prevention, wellness classes, etc.

**For all other marketing communications, a patient's written authorization is required**

---

# Continued Examples of Permitted Uses and Disclosures: Fundraising

- UCSD staff may only use demographic information (name, address, age, type of medical insurance) and dates of service for fundraising without authorization. (Disease, diagnosis or condition may not be used to develop a fundraising list.)
- UCSD staff must obtain a patient's written authorization to use any other PHI for fundraising
- All fundraising materials must provide the recipient with a way to **opt out** of receiving any additional fundraising material

**\*\*All fundraising efforts must be coordinated with  
the UCSD Health Science Development Office**

---

# Continued Examples of Permitted Uses and Disclosures: Research

- **De-identified PHI.** Aggregate data (stripped of all 18 identifiers) may be used and disclosed for research purposes without prior authorization, e.g., work preparatory to research / feasibility assessment
- **Limited Data Set of PHI.** With the removal of PHI direct identifiers (name, address, SSN, account number and other identifiers), a limited data set may be used and disclosed **if** a Data Use Agreement or another appropriate agreement is in place (e.g., between UCSD and the PHI recipient) and may require UCSD IRB approval
  - Limited data set may include “indirect identifiers” (dates, age, zip codes)
  - Contact the UCSD Research Compliance Office for assistance with the Data Use Agreement, [rcp@ucsd.edu](mailto:rcp@ucsd.edu) or 619-543-5841
- **PHI.** In order to access or use PHI or UCSD’s restricted databases for research purposes, the researcher must obtain appropriate IRB approval of the research protocol and the subject’s consent or an IRB waiver of authorization.

---

*Additional education on HIPAA privacy’s research requirements will be provided to individuals who also engage in research, <http://irb.ucsd.edu>*

# Continued Examples of Permitted Uses and Disclosures: Business Associates

- UCSD may disclose PHI to a 3<sup>rd</sup> party Business Associate to assist UCSD to do its job as long as a Business Associate Agreement (BAA) is in place
- Examples of “business associates”:
  - Medical transcription and billing vendors
  - Vendors assisting with medical account receivables
  - Attorneys, consultants, data aggregation services
  - Other vendors if they require access to PHI to assist UCSD with health care functions
- Refer requests for BAA agreements to the appropriate UC office for review and **authorized signature**, e.g., Purchasing, Contracting.

---

# All Other Uses of PHI Require Written Authorization

- HIPAA has very specific requirements for the written authorization. It must:
  - Describe the PHI to be released
  - Identify who may release the PHI
  - Identify who may receive the PHI
  - Describe the purposes of the disclosure
  - Identify when the authorization expires
  - Be signed by the patient / patient representative

---

# Examples of Circumstances when Patient Authorization is Required

- **Medical Records:**

- For the use and disclosure of medical information or records when that information is being provided / sent to someone other than the patient (e.g., patient's employer, friend, family, lawyer, accountant, etc.)

- **Media Communications:**

- For the use and disclosure to the media or for other types of external communications that contain PHI

- **Marketing and Other Products:**

- For the use and disclosure of a patient's PHI to pharmaceutical or medical device companies, non-profit organizations, etc.

- **Fundraising**

- For the use and disclosure of a patient's PHI, other than demographic information

# UCSDMC Authorization Form: General

- Form #151-036, "Authorization for Release of Protected Health Information (PHI)" is available at <http://health.ucsd.edu/his> or the UCSDMC Forms Management site (intranet): <http://forms.ucsd.edu/>

UNIVERSITY of CALIFORNIA, SAN DIEGO  
MEDICAL CENTER

Patient Identification \_\_\_\_\_

### AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

I authorize \_\_\_\_\_ to release health information to:

Name of person or facility, which has information \_\_\_\_\_

Name of person or facility to receive health information \_\_\_\_\_

Specify name/title of person to receive health information, if known \_\_\_\_\_

Street Address, City, State, Zip Code \_\_\_\_\_

(Telephone Number) \_\_\_\_\_ Extension: \_\_\_\_\_

**TYPE OF RECORD**

Medical                       Mental Health (other than psychotherapy notes)

**INFORMATION TO BE RELEASED**

Billing Statements       Emergency Medicine Reports       Outpatient Clinic Records  
 Consultations/Evaluations       Genetic Testing Information       Pathology Reports  
 Dental Records       History & Physical Exams       Progress Notes  
 Discharge Summary       HIV/AIDS Test Results       Psychological/Vocational Test Results  
 Drug and Alcohol Abuse Information       Laboratory Reports       Radiology and other Diagnostic Images (X-rays, etc)  
 EKG       Operative Reports       Radiology and other Diagnostic reports

Other \_\_\_\_\_

**SPECIFY THE DATE OR TIME PERIOD FOR INFORMATION SELECTED ABOVE:**

\_\_\_\_\_

151-036 (8-07)

UNIVERSITY of CALIFORNIA, SAN DIEGO  
MEDICAL CENTER

### AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

Patient Identification \_\_\_\_\_

**The purpose of this release is (check one or more)**

At the request of the patient/patient representative  
 Other (state reason) \_\_\_\_\_

**Notice**  
UCSD Healthcare and many other organizations and individuals such as physicians, hospitals and health plans are required by law to keep your health information confidential. If you have authorized the disclosure of your health information to someone who is not legally required to keep it confidential, it may no longer be protected by state or federal confidentiality laws.

**My rights**

- I understand this authorization is voluntary. Treatment, payment enrollment or eligibility for benefits may not be conditioned on signing this authorization except if the authorization is for: 1) conducting research-related treatment, 2) to obtain information in connection with eligibility or enrollment in a health plan, 3) to determine an entity's obligation to pay a claim, or 4) to create health information to provide to a third party.
- I may revoke this authorization at any time, provided that I do so in writing and submit it to:
  - Health Information Services  
UCSD Healthcare  
200 W. Arbor Drive, #8825  
San Diego, CA 92103-8825
  - Health Information Services  
UCSD Medical Group  
9350 Campus Point Drive, #0977  
La Jolla, CA 92037
- The revocation will take effect when UCSD Healthcare receives it, except to the extent that UCSD Healthcare or others have already relied on it.
- I am entitled to receive a copy of this Authorization.

**Expiration of Authorization**  
Unless otherwise revoked, this Authorization expires<sup>1</sup> on: \_\_\_\_\_  
(Insert applicable date or event)

**Signature**

\_\_\_\_\_  
(Signature of Patient or Patient's Legal Representative)                      Date: \_\_\_\_\_

\_\_\_\_\_  
(Printed Name)                      Time: \_\_\_\_\_ AM / PM

\_\_\_\_\_  
Relationship to patient (if other than patient):

**(Footnotes)**  
<sup>1</sup> If no date is indicated, this Authorization will expire 12 months after the date of signing this form.

---

# HIPAA Gives the Patient Specific Privacy Rights

- Patients have a right to request restriction of PHI uses and disclosures. Restrictions should not be granted by faculty or staff without consulting the Privacy Officer.
- Patients have a right to request confidential forms of communications (mail to the P.O. Box not street address, no messages on answering machines, etc.).
- Patients have a right to access and receive a copy of their medical record.
- Patients have a right to an accounting of the disclosures of their PHI.
- Patients have a right to request amendments to their medical record.

---

# Federal/State Privacy & Security Laws Require...

- Providers of health care to implement administrative, physical and technical safeguards to:
  - Ensure the confidentiality and privacy of medical information
  - Protect against reasonably anticipated threats or unauthorized uses or disclosures of PHI (45 CFR 164.306)
  - Safeguard patient medical information from unauthorized or unlawful access, use or disclosure
  - Implement policies and procedures to prevent, detect, contain, and correct security violations (45 CFR 164.308)

---

# Privacy / Security:

## Safeguards & Reminders

- Keep office(s) secured
- Password protect your computer
- Backup your electronic information
- Run updated anti-virus, anti-spam, and anti-spyware software
- Keep removable media (e.g., CDs, DVDs, USB attached drives) locked up
- In patient care settings, prevent ID theft by verifying the patient's identification at the time of service, e.g., driver license, passport, government issued photo ID
- Report privacy complaints and security incidents and... respond to incident reports promptly!

---

# Good Computing Practices:

## E-mail

- Don't open, forward, or reply to suspicious e-mails
- Don't open suspicious e-mail attachments or click on unknown website addresses
- Don't download unknown or unsolicited programs
- Delete spam

---

# Good Computing Practices:

## Passwords

- Use long, cryptic passwords that can't be easily guessed
- Protect your passwords -- don't write them down
- Never share your passwords

# Good Computing Practices:

## Workstation Security

- Physically secure your area and data when unattended
  - Encrypt files & portable devices containing restricted data (e.g., laptops, memory / USBs) to 128+
  - Secure laptop computers with a lockdown cable
  - Never share your access code, card or key
  - Lock your screen or log-off from restricted systems

*Locking your computer session is an easy way to prevent someone from accessing your computer when you step away. To "lock your computer session", press the CTRL-ALT-DEL buttons simultaneously, and select "lock session. At the Windows Security message, select "Lock Computer". If the Task Manager screen is displayed, select Shutdown -> Lock Computer. After locking your session in Windows, simply enter your windows password at the prompt to return to what you were doing.*

---

# Good Computing Practices: Portable Device Security

- **Don't keep confidential data on portable devices, unless it is absolutely necessary**
- Back-up data on portable devices to your department's secure server
- Encrypt (128+) and/or password protect all devices
  - *Encryption is a process that renders electronic information unusable, unreadable or indecipherable without the key.*
  - *To learn more about encryption, refer to the UCSDHS Compliance / Privacy web-site: <http://health.ucsd.edu/compliance/privacy.html>*

---

# Good Computing Practices: Data Management

- Know where PHI / restricted data is stored
- Destroy confidential data which is no longer needed
  - Shred or otherwise destroy restricted data
  - Erase information before disposing of or reusing drives
- Protect confidential and restricted data that you keep with back-ups to a departmental server

---

# Notice of Breach

## Federal / State Privacy Laws:

- Require licensed health facilities (clinic, hospital, home health agency, or hospice) to **prevent and report unlawful or unauthorized access** to, and use or disclosure of, patients' medical information. (Health & Safety Code 1280.15)
  
  - **Violations must be reported to:**
    - California Department of Public Health (CDPH) -- no later than **five days** after the unlawful or unauthorized access, use, or disclosure has been detected; and to the federal government.
    - Patients – notification of violation or breach, e.g., snooping, certain breaches of computerized data that contain unencrypted personal information about the patient.
  
  - The UCSD Privacy Office will co-ordinate notifications.
-

---

# Penalties

## ■ UCSD Policy:

- Employment sanctions and penalties may include corrective and disciplinary actions in accordance with UC policy up to and including dismissal / termination of employment.

## ■ State / Federal Privacy Laws:

- Agencies may assess fines and civil penalties against **any individual** or **provider of health care**
  - Penalties range from **\$2,500 - \$250,000** per occurrence (or higher), depending on the circumstances. Repeat violations and violations for financial gain are assessed higher penalties.
  - Violations may also be reported to the licensing board
  - California law permits civil suits against the individual
-

---

# Reporting Privacy and Security Breaches

- **UC policy states that any unauthorized access, use (including viewing) or disclosure of a patient's personal or health information is a violation of law and must be immediately reported.**
- **Examples of reportable incidents and violations:**
  - Any employee accessing patient information for non-work purposes
  - Loss / theft of computers, portable devices that contain unencrypted health information or personally identified information
  - Any loss / theft of medical records, films, etc.
  - Any complaints related to suspected identity theft or medical identify theft

# Reporting Privacy and Security Breaches

- All breaches must be reported immediately:

<b>UCSD Medical Center Information Security</b>	1-619-543-7474
<b>UCSD Health Sciences Privacy Office</b>	1-619-471-9150
<b>UCSD Hot Line</b>	1-800-403-4744 or <a href="http://universityofcalifornia.edu/hotline">http://universityofcalifornia.edu/hotline</a> Callers may be confidential or ask to remain anonymous.

---

# Questions about Privacy / Security?

- Kathleen Naughton, Director, Compliance / Privacy Program, UCSD Health Sciences
  - [knaughton@ucsd.edu](mailto:knaughton@ucsd.edu)
- Leland Giddings, M.D., Chief Compliance / Privacy Officer, UCSD Health Sciences
  - [lgiddings@ucsd.edu](mailto:lgiddings@ucsd.edu)
- Ken Wottge, Information Security Officer, UCSD Medical Center
  - [kwottge@ucsd.edu](mailto:kwottge@ucsd.edu)

# Confidentiality Statement

Web-link to UCSD Health Sciences Confidentiality Agreement, <http://health.ucsd.edu/compliance/hipaa.shtml>

- The protection of health and other confidential information is a right protected by law and enforced by individual and institutional fines, criminal penalties as well as UCSD policy. Safeguarding confidential information is a fundamental obligation for all employees, clinical faculty, house staff, students and volunteers.
- I understand and acknowledge that:
  1. I shall protect the privacy and security of confidential information at all times, both during and after my employment with the University of California has terminated.
  2. I agree to (a) access, use, or view confidential information to the minimum extent necessary for my assigned duties; and (b) disclose such information only to persons authorized to receive it.
  3. I understand that UCSDHS tracks all user IDs used to access electronic records. Those IDs enable discovery of inappropriate access to EITHER patient records or employee records.
  4. Inappropriate access and unauthorized release of protected information will result in disciplinary action, up to and including termination of employment, and will result in a report to authorities charged with professional licensing, enforcement of privacy laws and prosecution of criminal acts. The Office of Health Information Integrity (OHII) may levy penalties to **individuals or providers of healthcare** of **\$2,500 - \$25,000 per violation**.
  5. User IDs cannot be shared. Inappropriate use of my ID (whether by me or anyone else) is my responsibility and exposes me to severe consequences.

Print Name: \_\_\_\_\_ / Date: \_\_\_\_\_

---

# Certification of Training

- I have read the UCSD Privacy / Security training materials and confidentiality statement and agree to abide by UCSD policy and Federal / State privacy laws.
- Print name: \_\_\_\_\_
- Department name: \_\_\_\_\_ / UCSD
- Employee number: \_\_\_\_\_ <if known>
- Non-UCSD workforce member ID: \_\_\_\_\_
  - Indicate your date of birth and last 4 digits of your last name.