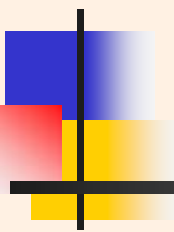


# Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rules



---

Education Module: HR/Benefits,  
Campus Benefits & Payroll

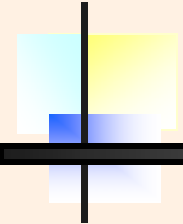
**Copyright © University of California**



# Why are we here?

---

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that the University train all members of its workforce about our HIPAA privacy-related policies and procedures before April 14, 2003.



# Objectives of this Training

---

To help you understand:

What HIPAA privacy rule is

Why it is important to you

Who must comply with HIPAA

When it starts

How HIPAA affects the work you do

Where to get help with HIPAA



# Objectives of this Training

---

- To meet requirements of law
- Training is mandatory



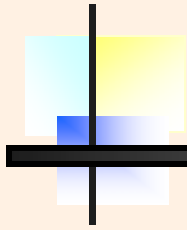
# What is HIPAA?

---

HIPAA is a federal law enacted to protect the privacy and security of an individual's

**Protected Health Information (PHI):**

- health information created or received by a health care provider, health plan, health care clearinghouse; and
- relates to the past, present or future physical or mental health or condition of the individual, the provision of health care to the individual or the payment for the provisions of health care; and
- identifies the individual.



---


Why does it affect our work in  
Human Resources, Benefits, or  
Payroll?



# Why it affects your work at UC

---

- UC health plans are covered entities;
- UC, on behalf of employees, may use or access PHI held by Health Plans;
- As an employee, you need to understand how HIPAA and other laws allow you to use, access, or disclose a member's health information.



Any and all protected health information that exists for any individual in any form:

---

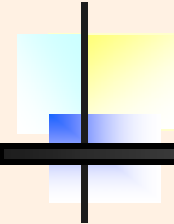
- Written
- Spoken
- Electronic



# University Health Plans are covered by HIPAA:

---

- The challenge is to understand the different requirements as sponsor, administrator, and employer
- As an employee of UC, you may have different responsibilities depending on the health plan

- 
- 
- Maria Faer, Ph.D.
    - HIPAA Privacy Officer for the University of California

# HIPAA has three Rules that affect the use & disclosure of health information

- The Privacy Rule: April 14, 2003 Compliance Date (Today's Discussion)
  - Reasonable security of physical records is expected under the Privacy Rule
- The Security Rule (for security of electronic records):
  - Rule published February 20, 2003 and compliance date is April 2005
- The Standardization of Transactions: October 2003 Compliance Date.
  - Touted as means of achieving savings and administrative simplification



# Principles of HIPAA

---

- Members have a right to know how their information is used (**Notice of Privacy Practices**)
- Members have a right to control the use and disclosure of their information (**Authorization**)
- Members have rights to access, amend, copy their information (**Patient Rights under HIPAA**)
- Covered entities bear the risk and responsibility for protecting the uses and disclosures of the information (**Only applies to Covered Entities**)
  - Civil and criminal fines and penalties for violations of HIPAA and current state privacy laws

# The Challenge and Risks for UC: Hybrid Covered Entity w/Two Covered Functions

---

- **Firewall Challenge & Risk:** Establish a firewall between covered functions and non-covered functions, even when carried out by same individual
  - Some of you wear multiple hats and carry out multiple functions
  - You cannot disclose PHI to non-covered entities or use PHI obtained in the plan sponsor role when you are wearing another hat
- **Perception Challenge & Risk:** Demonstrating that UC protects an individual's health information contacted in employee, student & research records even if that health information is not PHI and HIPAA-covered
  - Heightened focus on Privacy of all records due to HIPAA and the political environment
  - Heightened expectation that information should be protected even if not covered by HIPAA

# Who or what are HIPAA-Covered Entities?

---

- **Providers** of health care (treatment, diagnosis, palliative, preventative, rehabilitative, counseling, assessment with respect to physical, mental or functional status, etc.) who engage in electronic transactions (billing, claims, health care enrollment, etc.) are HIPAA Covered Providers
  - Providers of health care who do NOT engage in electronic transactions are called “uncovered providers,” but may choose to apply HIPAA to their activities
- **Health plans** are HIPAA Covered Entities
- **Health Care Clearinghouses** are HIPAA Covered Entities (processing of health information from nonstandard to standard format or vice versa between entities)
- **Business, finance, legal units** are HIPAA Covered Entities when they provide services to a covered provider, plan or clearinghouse

# Are you a HIPAA-covered entity?

## What “hat” do you wear and when?

---

- “The Provider Hat”--Are you a provider of health care services? **HIPAA-Covered.**
- “The Self-Funded Plan Hat”—Do you provide services to or for UC’s plans? **HIPAA-Covered.**
- “The Plan Sponsor Hat”—Do you handle an employee’s health plan information as employer-service? **Not HIPAA-Covered, but you have firewall responsibility.**
- “The Academic/Administrator Hat”—Do you handle a student’s health information in your role as administrator? **Not HIPAA-Covered, but you have firewall responsibility.**
- “Business and Finance Hat”—Do you provide services to the provider? Plan? Employer? Academic Units? Sometimes you are **HIPAA-Covered, and always have firewall responsibility.**

# All HIPAA-covered entities are part of UC's Single Health Care Component (SHCC)

---

*In May 2002, The Regents determined that:*

- UC is a HIPAA Hybrid Covered Entity
  - UC carries out both HIPAA covered and non-covered activities as health care providers, employer, and academic & research institution
  - Highly complex organization with the greatest potential costs and risks of compliance
- All covered entities (providers, plans and business & finance units) would implement a single system compliance program as the **UC Single Health Care Component (SHCC)**

# Benefits and Challenges of being a Single Health Care Component

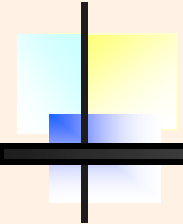
---

## ■ Benefits:

- Reduce costs of compliance and risks if UC were not internally consistent
- Enhance compliance with a plan that is workable for the academic institution
- Share health information within the single component for teaching and other health care activities without obtaining member's Authorization

## ■ Challenges:

- Implement HIPAA compliance requirements as a single entity—act like a “Single Health Care Component”
- Create a firewall between individuals and functions when there are multiple roles and multiple “hats”



---

Who within the University is  
responsible for complying with  
HIPAA?



# UC's Providers

---

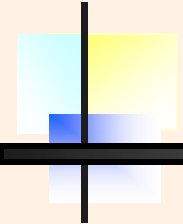
- Academic health centers
  - Medical centers
  - Some clinics, even if they are defined as “non-covered providers” have chosen to be part of the UC SHCC
  - Health professional schools and clinics
- Student Health Services
- Occupational Health and Medical clinics at Federal DOE labs administered by UC
- Clinics that are sponsored by UC academic departments and provide health care
- Individual faculty members, trainees and others who are part of the provider team



# UC's Self-Funded Plans

---

- High Option/Supplement to Medicare
- Core CA
- Core New Mexico
- BluePremier HMO
- BluePremier POS
- Health Care Reimbursement Account



# HIPAA covers Insured Medical Plans

---

- Health Net
- Kaiser Permanente California
- Kaiser Permanente Umbrella
- Kaiser Permanente Mid-Atlantic
- PacifiCare of California
- PacifiCare of Nevada
- Western Health Advantage
- Blue Cross PLUS
- Blue Cross PPO



# HIPAA covers non-medical Insured Plans

---

- Delta Dental
- PMI Dental
- Vision Service Plan



# HIPAA does not cover some non-medical plans

---

- Life Insurance
- Legal Plan
- Disability Insurance
- Accidental Death & Dismemberment Insurance

# OP Business and Finance Units that provide services to or for the Plans

---

- General Counsel
- Human Resources & Benefits
- Risk Management
- Accounting Services
- Audit
- President's Immediate Office
- Office of the Regents/Regents
- SVP Business & Finance
- Campus Payroll & Benefits Offices (including HCFs, EAPs, and CHROs)

# HIPAA is Federal Law that requires HIPAA-covered entities to:

---

- Protect the privacy and security of an individual's **Protected Health Information (PHI)**:
  - health information created or received by a health care provider, health plan, health care clearinghouse; and
  - relates to the past, present or future physical or mental health or condition of the individual, the provision of health care to the individual or the payment for the provisions of health care; and
  - identifies the individual.

# An individual's Health Information— HIPAA PHI or Not?

---

- PHI = Protected Health Information & **covered by HIPAA**
- IHI = individual's health information; may be in student academic & FERPA records or employee records; covered by state and federal laws (FMLA-related leaves), but **not covered by HIPAA**
- RHI = research health information that is used in human subjects research; protected by the Common Rule and other state or federal laws, but **not covered by HIPAA**

# Personal Identifiers under HIPAA include

---

- Name, all types of addresses including email, URL, home
- Identifying numbers, including Social Security, medical records, insurance numbers, biomedical devices
- Full facial photos
- Dates, including birth date, dates of admission and discharge, death

*Personal identifiers coupled with broad range of health, health care or health care payment information **creates PHI***

# Member's Privacy Rights

---

1. To receive a copy of the "Notice of Privacy Practices" (NPP)
2. To request alternative confidential communications
3. To request access to and copies of PHI in the DRS
4. To request an amendment / addendum to the DRS
5. To request an accounting of disclosures of PHI
6. To request restrictions or limitations on use / disclosure of PHI
7. Opportunity to agree or object—disclosures to family, friends; receive fundraising materials
8. To file a complaint of privacy practices

***A HIPAA Covered Entity MUST respond to all requests, although they may not be required to agree to all requests.***

# Pre-April 2003: Requirements of HIPAA Covered Entities

---

- Designate all covered entities & workforce members in the HR/Benefits (**document**)
- Designate individual responsible for the development & implementation of the policies & procedures (**document**)
- Complete business associate amendments or agreements (**document**)
- Develop policies & procedures that provide for the SHCC's compliance (**document**)
- Provide Training to all covered workforce members on those policies/procedures(**document**)
- Health Plan: Provide Notice no later than April 14, 2003
- Implement administrative, technical & physical safeguards

*Retain documentation for six years*

# Post-April 14, 2003 Requirements of Covered Entities

---

- Provide Notice of UC privacy practices to all members and make a good faith effort to obtain written acknowledgement of receipt (**document**)
- Obtain the individual's signed Authorization for uses and disclosures not otherwise permitted by the Privacy Rule (TPO) (**document**)
- Train all new employees and current employees when there is material change in job description (**document**)
- Assure that individuals responsible for responding to a member's request to exercise their HIPAA rights understand the requirements

# Covered Entities Must Provide Notice of Privacy Practices (NPP) to Member

---

## ■ By Health Plans

- At compliance date and at enrollment of new enrollees
- Every 3 years, must tell enrollees of Notice availability

## ■ The Notice describes

- Permitted & required uses / disclosures of PHI by CE
- Ability of the health plan to provide PHI to plan sponsor when the sponsor is carrying out its administrative functions
- Individual's rights (and how to exercise the rights)
- CE's legal duties with respect to PHI

## ■ Direct Treatment Providers must provide Notice

- No later than the date of first service delivery
- Make a good-faith effort to obtain written Acknowledgement of receipt of the Notice (document)
- Document if Acknowledgement not obtained
- Provide Notice as soon as reasonably possible in an emergency situation, but no Acknowledgement required

# Permitted and Required Uses and Disclosures of PHI

---

- To the individual (required)
- To DHS to investigate compliance (required)
- For Treatment (T), Payment (P), Health Care Operations (HCO)
- Incidental to a use or disclosure that is permitted
- Authorized by the individual
- To Business Associates (permitted)
- When individual does not have the opportunity to object and Authorization not required
  - Public health activities, law, health oversight, judicial and administrative proceedings, etc.
- When CE provides an opportunity for Individual to Agree or Object
  - Facility Directory, or Individuals involved in patient's care, or Disaster relief
- Creation of Limited or Deidentified Data Sets

# HIPAA Permits Use and Disclosure of PHI for Treatment, Payment & Operations (TPO)

---

- **Treatment** – The provision, coordination, or management of healthcare by one or more health care providers, including consultations and referrals
- **Payment** – Activities to obtain payment or be reimbursed for health care services; health plans to obtain premiums, fulfill coverage responsibilities, or provide reimbursement

The University's Notice of Privacy Practices describes the specific uses and disclosures for TPO



# HIPAA Permits Use and Disclosure of PHI for Treatment, Payment & Operations (TPO)

---

- **Health Care Operations (HCO)** -- Administrative, financial, legal and quality improvement activities; business activities; training, teaching; accreditation, credentialing, licensing, competence, performance activities; fraud, abuse, compliance activities
  - For UC's self-funded plans, payment activities are carried out by the University's TPA.
  - HIPAA requires UC to have a Business Associate agreement with the TPA (e.g., Blue Cross of California for Core & High Option/Medicare Supplement)



# Permitted Health Care Operations

---

- Customer service
- Resolution of internal grievances
- Case management and care coordination
- Reviewing the competence or qualifications of health care professionals, evaluating provider or health plan performance
- Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits
- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs
- Business management, planning and development
- Sale, transfer or merger of all or part of the CE
- Creating de-identified or limited data sets
- Conducting training programs
- QA and improvement activities

# Minimum Necessary Standard (MNS)

---

- Use or disclose only the minimum PHI that you need to know to do your job
- CE should have in place procedures that limit access according to job class, required use of PHI—“role-based access”
- Limit access, use or disclosure of PHI by others to the minimum amount necessary to accomplish the intended purpose
- A “think twice” standard:
  - Is it reasonable?
  - Is it necessary?

# Minimum Necessary Standard

## -- Exceptions

---

- Disclosures to providers for treatment
- Disclosures to the individual member
- Uses /disclosures with an authorization
- Uses /disclosures required for HIPAA standard transactions
- Uses /disclosures required by law
- Disclosures to HHS/OCR for enforcement

# A Covered Entity must obtain the Member's signed Authorization

---

for:

- Health Plans may require for disclosures to Benefits Representatives or Health Care Facilitators
- Release of PHI to other third parties for purposes other than HIPAA
  - Marketing, media
  - Release of Mental Health Records & Psychotherapy Notes
- Research
- Employee may authorize release of PHI for employment-related decisions (e.g., ADA, FMLA, etc.)
- Others

# Authorization Form Requirements:

---

## ■ Elements

- Description of PHI and purpose of disclosure
- Name of person (s) or class of persons authorized to receive PHI
- Expiration date / event
- Signature of member (or personal rep.) and date
- If personal rep signs, state relationship to member
- Disclosure of any direct or indirect remuneration

## ■ Required Statements:

- Right to refuse to sign and Right to revoke
- CE may not condition treatment, payment, enrollment or eligibility for benefits
- Potential for re-disclosure of disclosed information

## ■ Other requirements:

- Plain language
- Copy to the individual
- Retain for 6 years



# How does HIPAA affect you and your job requirements?

---

- Self-funded “Hat” and responsibilities
- Employer and Plan Sponsor “Hat” and responsibilities
- Other Business and Finance Roles and Responsibilities
- In all cases, we must be mindful of the HIPAA requirement to obtain Authorization when PHI flows outside of the covered entity, unless permitted or required by federal and state law

# What are the responsibilities of the UC's self-funded Health Plans?

---

- Provide Notice by 4/14/03 to all members of the plan's privacy practices
  - Notice should state that the Health Plan may disclose PHI to the Plan Sponsor
  - Notice must describe how the employee may exercise individual rights
- No written Acknowledgment required
- May disclose PHI to another covered entity or any health care provider for the payment activities of the entity
- May disclose PHI to a provider for treatment activities

# What are the responsibilities of the UC Self-Funded Plans?

---

- May disclose PHI to another covered entity for certain health care operations of that entity if both have had a relationship with the member
- May disclose summary health information to the plan sponsor
- May disclose PHI to the plan sponsor to carry out plan administration functions
- Do not disclose PHI to the plan sponsor for the purpose of employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the plan sponsor
- Respond to requests for confidential communications

# What are the responsibilities of UC, the employer and plan sponsor?

---

- Establish the plan administration functions performed by the plan sponsor and separate those functions from all other employer-role activities
- Amend the plan documents
  - Establish permitted and required uses & disclosures by plan sponsor and adequate separation between plan sponsor and health plan
  - Identify UC employees under control of the plan sponsor who have access to PHI and restrict access to PHI to plan administrative functions
  - Make information available to provide for accounting of disclosures, and respond to requests to access and amend
  - Certify to the health plan that UC the plan sponsor will restrict uses and disclosures of PHI as described in the amended plan documents
  - PHI must be protected in the same manner as when UC is the plan administrator

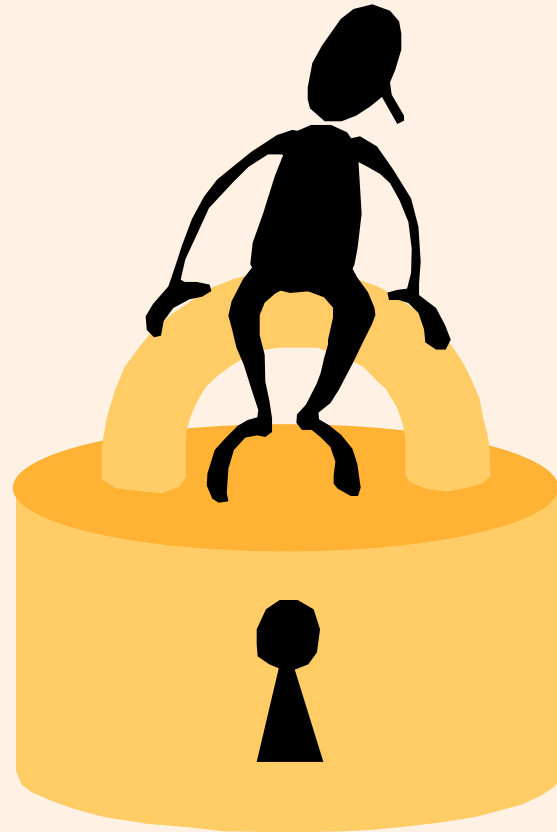


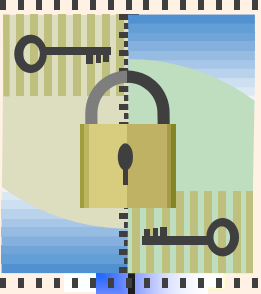
# Privacy Officers

---

- Role of Privacy Officer
- Role of Designated Privacy Officers

# HIPAA also requires Security





# It's Good to Know: Privacy & Security Go Hand-in-Hand

---

- Privacy focus is – “Who can access, use or disclose information?”
  - “What is Private?” is key concept.
  - Patient’s rights to know how information is used and disclosed
  - Patient’s right to control access to information
- Security focus is – “How do we keep it private?”
  - Privacy Rule - protects security of information in all forms
  - Security Rule - protects electronic information



# HIPAA – Security Tips

- Security of electronic data: **Your responsibility!**
  - Password security is key...NEVER SHARE PASSWORDS
  - Password protect your PCs, PDAs, laptops, home computers; use automatic log-offs
  - Secure access, transmission, storage and retention of e-data
  - Don't leave confidential information on your computer screen, or in the trash! Develop procedures to reasonably safeguard information transmitted by email.
  - Use caution when sending faxes. Be aware of who may be viewing the information from both fax machines. Use fax cover sheets and verify fax #s.
  - Report breaches to your UC privacy / security officer.
- Physical security of data: **Your responsibility!**
  - Do use locked shredder bins.
  - Key access to file rooms / cabinets

# Consequences of Non-Compliance

---

- Misuse of health information: fines up to \$50,000 and/or prison sentence up to one year
- Misuse under false pretenses: fines up to \$100,000 and/or prison up to five years
- Misuse with intent to use health information for commercial advantage, personal gain or malicious harm: fines up to \$250,000 and/or prison up to ten years
- California law also imposes strict penalties for violations of California privacy laws
- HIPAA violations could place a provider's license, an employee's job, or professional credibility at risk, and could lead to trials and damaging publicity for individuals and institutions

# Suspected or known violations: Individual and Institutional Responsibility

---

- You have a responsibility to report known violations, including unintentional errors or mistakes, so that the University can take immediate action to correct or mitigate harmful effects
- The SHCC must have in place a process to mitigate violations, both unintentional and willful
- The SHCC must have in place a process to receive and respond to complaints

# Understand your individual responsibility

---

- Always maintain a separation between your covered and non-covered activities and know what additional state or federal laws apply to the privacy of an individual's health information
- Never disclose PHI to other non-covered entities (UC or third parties) without Authorization or unless required or permitted by law
- Always apply the minimum necessary standard to uses and disclosures of PHI

# Understand your individual responsibility

---

- Understand when you can use and disclose PHI and the requirements that apply to those uses and disclosures for:
  - Health care operations
  - Health care payment
  - Exchanges with a provider for treatment purposes
  - If questions, see the University's Notice(s) of Privacy Practices or the definitions in the regulations
- Determine when a Business Associate Agreement is required—when a contractor or vendor uses or discloses PHI for or on behalf of the covered entity



# Your individual responsibility

---

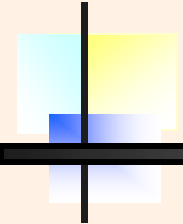
- Seek help when you don't know if you are allowed to use or disclose PHI
  - Office of the General Counsel
  - University Privacy Official or Contact Office
  - Campus or Hospital Counsel or Privacy Officers
- Obtain the required training
- Use the reference materials
  - UC Systemwide Standards and Policies
  - UC Notices of Privacy Practices
  - HIPAA Privacy Rule
  - Training Modules



# HIPAA is really very simple:

---

We want to protect the privacy of our members by safeguarding our use and disclosure of protected health information

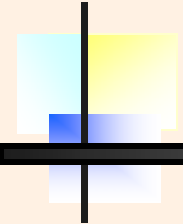


HIPAA gets complex when we try  
to determine what hat we are  
wearing:

Plan Administrator

Plan Sponsor

Employer



Always treat  
individually identifiable health  
information

---

as

Protected Health Information (PHI)



## HIPAA means...

---

it is unlawful to share this  
information inappropriately



# Three things to remember

---

When performing tasks related to UC's role as plan sponsor or plan administrator—

# 1. HIPAA says

It's OK to use PHI for:

---

- Treatment
- Payment
- Operations



2. If an activity involves PHI,

---

Use or Disclose only

the **MINIMUM NECESSARY**



# Use the “Think Twice Standard”

---

Is it reasonable?

Is it necessary?

### 3. Maintain an absolute FIREWALL between

---

Your activities for the health plan and any employment-related activities or decisions

# Carriers, departments, and campus offices can use or disclose information necessary to

---

- resolve problems with treatment, payment and operations (TPO) and to carry out our responsibilities to administer the plan or resolve member's payment or eligibility problems
- Whether plan is self-insured or insured, we are allowed to exchange PHI according to HIPAA rules for TPO



# Payment, eligibility, and other problems:

---

- Member provides her member number, ID, plan, claim number, what claim was for and date of service.
- When we call the carrier we need the member number, ID, plan, claim number, date of service
  - What claim was for may not be necessary, but is permitted by HIPAA.



# Payment, eligibility, and other problems

---

- Must protect the PHI provided by member and not use for any other purposes



# Simple Do's

---

- **DO** “Think Twice” before sharing PHI
- **DO** Refer problems to your supervisors or your local Privacy Officer
- **DO** Keep records and communications secure:
  - Fax
  - Email/voice messages
  - Paper records locked away and off desktop



# Simple Don'ts

---

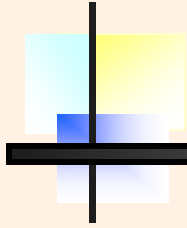
- **DON'T** use or disclose PHI for employment-related functions;
- **DON'T** Leave voice mail with PHI;
- **DON'T** Share computer or system passwords;
- **DON'T** Leave PHI on your computer screen or desktop.



# To comply with HIPAA

---

- Look at your operations and procedures and make them compliant:
  - Files, fax, phones, messages, mail
  - Record keeping (lock them away)
  - What you say to whom
  - How you exchange PHI when it is necessary
  - Maintain the firewall



What is the minimum necessary?



# So....

---

Member calls and volunteers PHI in order to communicate the urgency of his problem:

- Be polite and listen
- If he asks if PHI helps, "Think Twice"
- Document the call--including the PHI, if relevant
- When referring the call information to another department or the carrier, pass along only the minimum necessary



# Case #1

---

Member calls Customer Service about a prescription problem:

- Prescription for her husband
- Heart condition



# Member could be calling because

---


- Eligibility problems--they were told they are not covered
- There might be limit issues with the medication
- They need a prior authorization and were denied



# Scenario 1: We verify eligibility on our systems

---

- Print the screens
- Fax them to the plan
- OK?



Carrier FAX machine must be secure and cover page should have a confidentiality statement

- Use only secure fax numbers
- List of safe fax numbers
- Verify security procedures



# What do you do with the material after your fax is sent?

---

- Once PHI is no longer needed, it should be properly destroyed



## Scenario 2: To resolve the problem

---

Call the plan to discuss the problem;

Exchange PHI only when required to do your job

Remember: **MINIMUM NECESSARY**



# Plan representative is not there

---

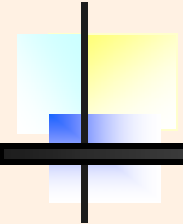
- Do you leave a message on her voice mail?
  - Not if you don't know that it is secure/password protected voice mail
  - If on the list of secure/password protected voice mail, OK.

When resolved, you try to call the  
member

---

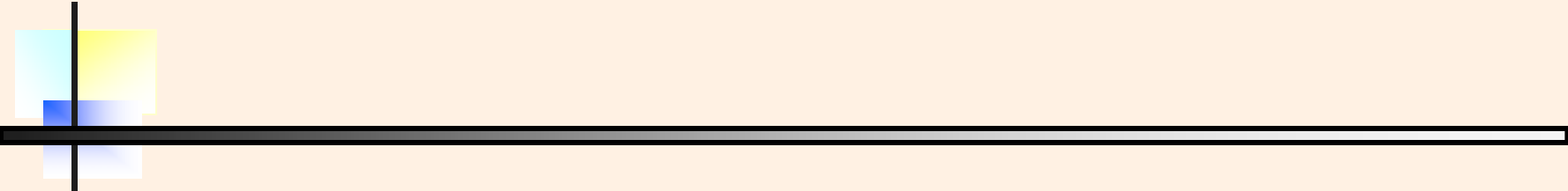
He is not home...

Do you leave a message?

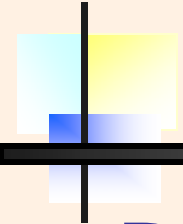


---

What if the message on the answering machine doesn't identify you have the right party?

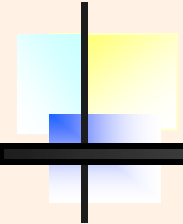


“This is Joe Navoa from UC Customer Service calling to confirm your issue has been resolved. If you have any questions, call me Monday – Friday, 9-4.”



---

Do not include the name, the plan, the social security number, the ailment, problem or resolution specifics



# Member said leave a message:

---

Answering machine identifies it is the right party

“Think Twice” & minimum necessary

Leave the same message

# HIPAA is just a new way of thinking about personal information

---

In some instances, it changes what we  
can do, ...but it is not difficult



# It's also a matter of respect

---

If you were the member, how would you want people to handle it?



# Remember

---

- Always maintain a separation between your covered and non-covered activities and know what additional state or federal laws apply to the privacy of an individual's health information
- Never disclose PHI to other non-covered entities (UC or third parties) without Authorization, unless required or permitted by law
- Always apply the minimum necessary standard to uses and disclosures of PHI



# This is only the beginning

---

HIPAA compliance begins no later than  
April 14, 2003;

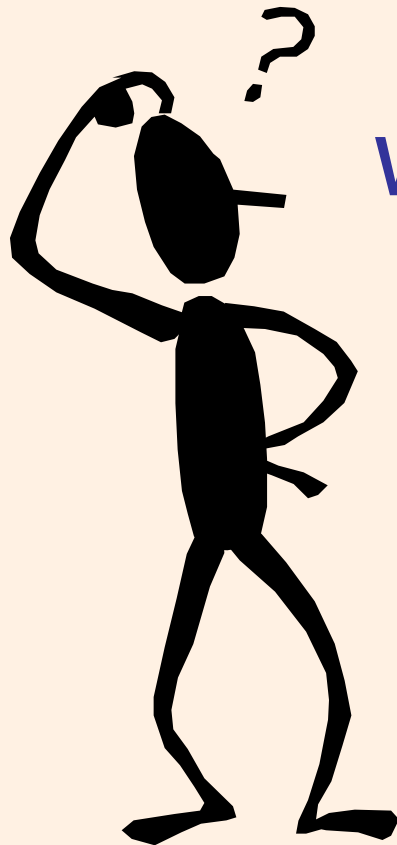
More to come with Standards of  
Transactions, October 2003

Security & Electronic Standards in 2005



---

If you have questions



where do you go?

# Website

# http://AtYourService.ucop.edu

The screenshot shows a Microsoft Internet Explorer browser window displaying the 'At Your Service' website. The browser's address bar shows the URL 'http://atyourservice.ucop.edu/'. The website header includes the title 'At Your Service' and the subtitle 'University of California • Human Resources and Benefits'. A navigation menu at the top right contains links for 'Contact List', 'Site Map', 'Forms & Publications', and 'Search'. Below this, there are tabs for 'Employees', 'Former Employees', 'Annuitants', and 'Administrators'. The main content area features a large heading 'I have an employee question about...' with a photograph of a man and a woman. To the right of the photo are four dropdown menus for 'Life/Work Changes', 'Health & Insurance', 'Retirement & Savings', and 'Personnel Policies, Contracts, & Procedures'. A search box with a 'Search' button is located to the right of these menus. Below the photo is a 'Current News' section with a 'Browse News Archive' link. Three news items are listed: 'UCRS Semi-Annual Account Statement Mailing for December 31, 2002' (February 28, 2003), 'Frequently Asked Questions About CAP II' (February 25, 2003), and 'Questions and Answers about UC's budget and its impact.' (January 29, 2003). On the right side of the page, there is a vertical column of blue buttons with white text: 'Your Benefits Online', 'New Employees', 'Labor Relations', 'Retirement Calculators', 'Retirement Plans Values & Performance', 'Job Seekers', 'Change Address/Payroll Information', and 'Lost PIN / Change PIN'. The footer of the website contains the text 'University of California - Human Resources and Benefits' and several links: 'At Your Service', 'UCOP HR/Benefits', 'UCOP Home', 'Terms of Use', and 'How to Use This Site'. The UC logo is also present. The browser's taskbar at the bottom shows the Start button, several open applications (Eudora, Microsoft PowerPoint, neo - CD La...), and the system tray with the date and time '11:54 AM'.



# Conclusions

---

- 1. HIPAA affects the work we do because we provide customer service to members and administer the health plans;
- 2. HIPAA places a focus on privacy—new expectations and new rights;
- 3. Members may test those rights—we must respond



# If members have questions

---

- Regarding rights under HIPAA, they should be referred to:

UC Health and Welfare Plans Privacy  
Office, 300 Lakeside Drive, 5th Floor,  
Oakland, CA 94612



# Conclusions

---

- 4. HIPAA is absolutely clear—can't use or disclose your knowledge working with the health plans to make employment-related decisions
- 5. The University's notice describes how we may use or disclose PHI. Familiarize yourself with the Notice.

# Questions & Answers

---

