Please use your cell phone to access this website:

pollev.com/ucsfprivacy
Privacy and Confidentiality
Residents and Fellows Orientation 2015

Deborah Yano-Fong, RN, MS, CHPC
Chief Privacy Officer
Overview

• Why is This Important?
• State and Federal Privacy Laws and Regulations
• Five Things To Remember
• What is Your Responsibility?
• Privacy Concepts and Best Practices
Why Is This Important?

• Welcome to California ....

Be Aware:

– Financial consequence to you, and the hospital/organization
– Professional license impact
# State and Federal Privacy Laws and Regulations:

<table>
<thead>
<tr>
<th></th>
<th>Fines</th>
<th>Criminal Penalties</th>
<th>Civil Penalties</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Up to $250,000</td>
<td>Misdemeanor</td>
<td>Damages plus $1,000 fine per patient</td>
</tr>
<tr>
<td>Federal</td>
<td>Up to $1.5 million</td>
<td>Up to 10 years in prison</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## More Headlines To Avoid

<table>
<thead>
<tr>
<th>Patients Impacted</th>
<th>78.8 Million Patients</th>
<th>Anthem Blue Cross</th>
<th>2/4/2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Largest HIPAA Fine</td>
<td>$4.8 Million</td>
<td>Columbia Medical Center</td>
<td>9/27/2010</td>
</tr>
</tbody>
</table>
### Survival Tips For HIPAA Patient Rights

#### For Patient Requests:

<table>
<thead>
<tr>
<th>DO NOT</th>
<th>Agree to requests for restriction/amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO</td>
<td>Refer patient to Patient Relations or HIMS</td>
</tr>
</tbody>
</table>

#### For Research Data:

<table>
<thead>
<tr>
<th>DO NOT</th>
<th>Harvest research data from any Medical Record source yourself</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO</td>
<td>Go to HIMS/Integrated Data Repository. Review Policy 5.01.06 “Control of Access to and Release of Info…”</td>
</tr>
</tbody>
</table>
Please use your cell phone to access this website:

pollev.com/ucsfprivacy
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser
Correct Answer to Scenario #1 is E

• You should not be accessing the record at all

• Remember:
  – Accessing APeX is only for UCSF business
  – Accessing your significant other’s record is not part of your UCSF duties
  – APeX access is tracked and monitored

• Consequence for Inappropriate access:
  – Potential disciplinary action, up to and including termination of employment, loss of your professional license, and civil and criminal penalties
Five Things To Remember:

1. Minimum Necessary
2. Encrypt Every Electronic Device
3. When in Doubt, call the Privacy Office
4. Electronic Safeguards
5. Physical Security
1: Minimum Necessary Standard

Applies for all uses and disclosures except for treatment

- Payment and Healthcare operations
- Access only what you need to know
- Share only what you need to disclose
Scenario #2

Situation:

- Resident
- Personal laptop
- Check my UCSF email
- Never save PHI onto my laptop.
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser
Correct Answer to Scenario #2

B. Yes, because I access my UCSF email, which may result in files automatically downloading to my laptop without my knowledge

• Your laptop must be encrypted. Accessing UCSF email from your personal laptop may result in your UCSF data, mail and attachments being automatically downloaded and stored on your device. Thus, encrypt your personal device before using it for UCSF business.

• If the encrypted device is lost or stolen, the information in it (both personal and UCSF) is secure and inaccessible to thieves.
2: You Must Encrypt

If you use the computing or electronic devices for UCSF business:

- **Devices include:**
  - Desktop computers
  - Laptop computers
  - Smart phones (e.g., iPhone, Android, Blackberry)
  - Tablets (e.g., iPad)
  - External drives (e.g., USB flash drives)

- **UCSF business purposes include:**
  - Checking UCSF email
  - Accessing the network via VPN
  - Accessing or storing UCSF information

- **FYI:** Encryption does not perceptibly slow down your computer
3: When In Doubt, Call the Privacy Office

UCSF Privacy Office

415-353-2750
4: Electronic Safeguards

- Inventory the devices you are using for UCSF business (even if it’s just to check UCSF email)
- Use the following UCSF guidelines to encrypt your personal devices
  - Desktops/laptops: http://tiny.ucsf.edu/9bTkaB
  - Smartphones: http://tiny.ucsf.edu/H4mMrU
- Contact the IT Service Desk at (415) 514-4100 for encryption questions
Electronic Safeguards: Secure Email

• How To Use Secure Email at UCSF
  • Include the trigger word followed by a colon in the subject line:
    Secure: ePHI: PHI:
  • Make sure you are sending your message to the correct recipient
  • Do not include PHI in the subject line

• Remember
  • This protects the information when it leaves our UCSF network environment. It does not encrypt the message within the UCSF network, as our internal network is secure. However, best practice is to always use secure email as this will protect you if someone forwards your message outside of the UCSF network.
5: Physical Security

• Do not take paper documents containing confidential UCSF information offsite, including:
  – Protected health information (PHI)
  – Personal identifiable information (PII)
  – Human subjects research information

• Instead of taking documents offsite:
  – Login to UCSF systems using VPN on an encrypted device
  – Securely email documents to yourself
  – Save files to an encrypted device
Physical Security

• If you must take hard copy UCSF information offsite:
  – De-identify the information as much as possible
  – Secure and keep it on your body at **ALL TIMES**
    • Locking documents and devices in your vehicle’s trunk or glove compartment is NOT secure and is a target for thieves
  – Destroy the documents as soon as they are not required
## What Do I Do If Something Goes Wrong?

Report incidents immediately:

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Who To Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misdirected PHI</td>
<td>Privacy Office</td>
</tr>
<tr>
<td>Verbal Disclosure</td>
<td>Privacy Office</td>
</tr>
<tr>
<td>Lost or Stolen Electronic Device</td>
<td>Privacy Office, IT, and UCSF PD</td>
</tr>
<tr>
<td>Inappropriate Access</td>
<td>Privacy Office</td>
</tr>
<tr>
<td>Research Incident</td>
<td>Privacy Office and CHR</td>
</tr>
</tbody>
</table>

_OOPS!_
Best Privacy Practice Summary

1. Minimum Necessary Standard
2. ENCRYPT all mobile & electronic devices
3. WHEN IN DOUBT – CALL THE PRIVACY OFFICE
Best **Privacy** Practice Summary Cont.

4. **Electronic Safeguards**
   a. Do not block software upgrades
   b. Do not email spreadsheets with patient information

5. **Physical Security**
   a. Place paper PHI in confidential shredding bin
   b. Do not take hard copy PHI off-site; if you must, keep it on your body at all times
   c. Carefully verify each document you give to patients/families to ensure it is for the correct patient (2 identifier verification for mailing, faxing, etc.)
   d. Limit discussion in public areas
UCSF Privacy and Compliance in a Nutshell

• This presentation is an overview of privacy and security. For more information refer to:
  – UCSF Confidentiality Handbook
  – Privacy Office Website – hipaa.ucsf.edu
  – Call the Privacy Office – 353-2750
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser
Correct Answer to Scenario #3

D. “No, I cannot photograph this patient because I do not have consent to do so.”

Even without the face, the photo may reveal a unique characteristic (e.g., tattoo), or the patient’s traumatic accident made headlines, in which the photo may reveal the patient’s identity.

You must obtain consent from the patient/patient’s representative for any photography or filming of the patient for non-treatment purposes.