Privacy and Confidentiality
Residents and Fellows Orientation 2013
Deborah Yano-Fong, RN, MSN, PAAPC, CHP
Chief Privacy Officer

Overview
- What Do You Need to Know?
- Laws and regulations
  - California Privacy State Laws
  - Federal Regulations: HIPAA, HITECH & Final Omnibus Rule
- Important Privacy Concepts
- Privacy in the Clinical Environment
- Case Studies
- Best Privacy Practice Reminders
- What to do in the Event of a Privacy Breach?
- Resources

What do you need to know about Privacy and HIPAA?
- Complete the required training
  - Privacy Handbook
  - Confidentiality Statement
- Know the patient’s privacy rights
- California state privacy laws and your personal liability
- American Recovery and Reinvestment Act (ARRA) impact on healthcare and privacy – HITECH and Final Omnibus Rule

Advanced Provider HIPAA Training and Basic HIPAA Training
- This session covers
  - Advanced Provider HIPAA Training
  - Research Training
  - Both training modules can be found at http://hipaa.ucsf.edu/education
- Privacy and Security Survival Tips
- Notice of Privacy Practices (NPP)
  http://www.ucsfhealth.org/pdf/3-03ucsfhipaa.pdf

Patient HIPAA Rights can be Hot Spots for Providers
HIPAA Patient Rights:
- To restrict use and disclosure of their PHI
  - Self-pay
- Amendments
- To file complaints with UCSF, UCOP, and OCR
  - May result in civil and criminal penalties for individuals as well as the healthcare organization
- Accounting of Disclosures
- Copy of medical record
  - Right to receive an electronic copy
- Confidential communications

Survival Tips For HIPAA Patient Rights
Do Not:
- Agree to requests for restriction or amendments
- Harvest research data yourself from any of the Medical Record sources. HIMS is the control point for providing research data. For questions go to http://hims.ucsfmedicalcenter.org or go to the IDR (Integrated Data Repository)

Do:
- Refer patient to Patient Relations or HIMS
- Patient Relations and HIMS evaluates and coordinates all restriction or amendment requests
What's New?

Privacy is more than HIPAA these days
- State laws and federal regulations are more stringent and impose increased fines and penalties
- The privacy environment is constantly changing and is more complex
- Initiatives for Health Information Exchanges (HIE)
- Proliferation of disease registries

Major Impacts of The California State Privacy Laws:

<table>
<thead>
<tr>
<th>Civil Code 56.36/Health &amp; Safety Code 130200</th>
<th>Health &amp; Safety Code 1280.15</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mandates the confidentiality of medical information</td>
<td></td>
</tr>
<tr>
<td>• Implement appropriate administrative, technical and physical safeguards to protect the privacy of a patient's medical information, and implement reasonable safeguards to prevent unauthorized access, use, or disclosure.</td>
<td></td>
</tr>
<tr>
<td>• Mandates prevention of unlawful or unauthorized access to, use of, or disclosure of patient medical information</td>
<td></td>
</tr>
<tr>
<td>• Reporting obligations</td>
<td></td>
</tr>
<tr>
<td>• Incident of unlawful access, use, or disclosure of a patient's medical information must be reported within 5 days of detection of the breach to CDPH and the affected patient(s) / legal representative.</td>
<td></td>
</tr>
</tbody>
</table>

Major Impacts of The CA Privacy State Laws:

<table>
<thead>
<tr>
<th>Civil Code 56.36/Health &amp; Safety Code 130200</th>
<th>Health &amp; Safety Code 1280.15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Fines / Penalties:</td>
<td></td>
</tr>
<tr>
<td>• $2,500 – $25,000 per violation</td>
<td></td>
</tr>
<tr>
<td>• $250,000 – maximum penalty</td>
<td></td>
</tr>
<tr>
<td>• Potential for civil action by consumer with statutory damages ($1000) in addition to actual damages</td>
<td></td>
</tr>
<tr>
<td>• Cal-Ohl may notify licensing board for further investigation/discipline of individual providers.</td>
<td></td>
</tr>
<tr>
<td>Institutional Fines for failure to prevent or report:</td>
<td></td>
</tr>
<tr>
<td>• $25,000 – initial violation (per pt.)</td>
<td></td>
</tr>
<tr>
<td>• $17,500 – subsequent occurrence</td>
<td></td>
</tr>
<tr>
<td>• $250,000 – maximum penalty</td>
<td></td>
</tr>
<tr>
<td>• $100 / day for late reporting</td>
<td></td>
</tr>
<tr>
<td>• Criteria considered by CDPH included in the determination of amount of the fine.</td>
<td></td>
</tr>
<tr>
<td>• CDPH may refer violation to CalOhl</td>
<td></td>
</tr>
</tbody>
</table>

Impact of Federal Laws & Regulations

HITECH Act and the Final Omnibus Rule amend HIPAA
- "Stimulus Package" included health information technology, e.g., Electronic Health Records
  - Defines unsecured PHI
  - Encryption of laptops & other devices is a must
  - Increases criminal fines and penalties
  - Right of civil action for wrongful disclosure up to $1.5 M
- How Does This Impact You?
  - Surveillance and Monitoring

Newspaper Headlines

• In September 2012, Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. ("MEEI") agreed to a $1.5 million settlement with the Office for Civil Rights over a theft of an unencrypted personal laptop containing PHI of MEEI patients and research subjects.

Important Privacy Concepts

• Utilize these concepts when making decisions regarding Privacy Protection in the clinical environment:
  - Treatment, Payment or Operations (TPO)
    - You may access, use, or disclosure PHI or ePHI for TPO purposes
    - Refer to Notice of Privacy Practices (NPP)
    - If your access, use or disclosure is not covered by the NPP, then you will need to obtain Patient Authorization prior to proceeding.
Important Privacy Concepts (cont.)

- How To Use Secure Email at UCSF
  - Type in the email subject line the trigger word: Secure: ePHI: PHI:
  - Make sure you are sending your message to the correct recipient
- 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.

Scenario #1 – Access to Clinical Systems

- You are interested in conducting a retrospective research study and need research subject clinical data
- Since you have access to UCSF clinical systems, can you access the clinical data of your patients for use in your research study?

Scenario #1 – Answers

A. Yes
B. No

Correct Answer to Scenario #1

B. NO
You may only access UCSF’s clinical systems for purposes of Treatment, Payment and Healthcare Operations (TPO).
In order to obtain clinical data for research purposes, the study must have CHR (IRB) approval and the data must be requested from HIMS or the Integrated Data Repository (IDR).

What if your personal, unencrypted laptop was stolen?
Scenario #2 - Lost / Stolen Laptop

- Your personal laptop contained information about your patients. The laptop was locked in your trunk and it had a complex password.

- Since you locked the laptop up and you had a complex password on the device, is this enough to keep you from being personally responsible for the loss of patient information?

Scenario #2 - Answers

A. Yes, I cannot be responsible if someone steals my laptop.

B. No, I am still responsible.

Correct Answer to Scenario #2

B. “No, I am still responsible.”

The only safe harbor is to ENCRYPT your device.

Note: You may be personally responsible for civil and monetary penalties associated with the incident, and your license may be impacted.

Scenario #3 – Social Media

- You are very upset because a young patient of yours has just coded and was not able to be resuscitated. You want to share this experience and your thoughts and feelings with your family and friends on Facebook. What must you consider before doing this?

Scenario #3 – Answers

A. Posting this on Facebook is OK as long as you do not identify the patient by name, or identify the hospital, and you are limiting the recipients to your friends and family.

B. You cannot post anything on Facebook that could possibly lead to identification of the patient.

Correct Answer to Scenario #3

B. You may not post anything on Facebook that could possibly lead to identification of the patient.

Facebook is considered public domain, and anything you post there is considered public information. Posting clinical details is a violation of your patient’s right to privacy and confidentiality without authorization. Your Facebook profile may identify your place of work and your occupation. When linked with your posting, this provides additional details that may identify the patient. Information you obtain from your patient/provider relationship is confidential.
PHI is Everywhere

- Desktop computer
- Laptops
- Memory Sticks
- Text pagers
- iPads/tablets
- Cell Phones
- Conversations
- Paper records/notes

Best Privacy Practice Reminders

- ENCRYPT all mobile & electronic devices
- Do not leave PHI / ePHI unattended or unsecured; use cable locks to secure devices or secure them in locked cabinets
- Limit discussion in public areas
- Carefully verify each document you give to patients/families to ensure it is for the correct patient
- Place PHI / ePHI in confidential shredding bins
- Do not block software updates

Protect your computers and mobile eDevices:

- Encrypt everything
- Regularly backup all confidential information
- Use complex passwords
- Delete old files
- Access UCSF network using an approved, secure means, such as VPN

What is my responsibility?

Report immediately:

- To the Privacy Office: any known or suspected privacy breaches
- To IT: erratic computer behavior or unusual e-mails
- To UCPD: lost or stolen electronic devices or UCSF information

Scenario #4 - Photography

- You are rotating in the ED and see a deceased patient with an amputated leg.

- Can you take a photo of this patient’s leg and share it with your colleagues?

Scenario #4 - Answers

A. Yes, because the patient is deceased.
B. Yes, because my colleagues are also healthcare providers.
C. Yes, because the patient’s face is not in the photo.
D. No, I cannot photograph this patient because I do not have consent to do so.
Correct Answer to Scenario #4

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.

Remember - Privacy is bigger than HIPAA
Privacy answers are not black & white

- California Confidentiality of Medical Information Act (CMIA) (CA Civil Code 56-56.07)
- California Confidentiality of Social Security Numbers (CA Civil Code 778.55)
- California Information Practices Act (IPA) (CA Civil Code 1798.12)
- California Lanterman-Petris-Short Act (CA Welfare and Institutions Code 4500-5120)
- Federal Education Rights and Privacy Act (FERPA) (34 CFR Part 99)
- Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR Parts 160, 162, 164)
- AB-211
- SB-541
- Red Flag Rule
- HITECH

UCSF Resources
Where to go for help

- Your Chief/Chair/Department Manager or IT support person
- UCSF Chief Privacy Officer
  - Deborah Yano-Fong
- UCSF Information Security Officer (Medical Center)
  - Rob Winter
- UCSF Information Security Officer (Campus)
  - David Rusting
- School of Medicine Chief Technology Officer (SOM ISU)
  - Opinder Bawa
- IT Customer Support
  - 514-4100
- UCSF Police
  - 476-1414