Professional Conduct

Orientation Topics for New Medical Students
Compliance vs. Ethics, Code of Conduct, Privacy & Security
UC San Diego Health Sciences

Kathleen Naughton
Chief Compliance / Privacy Officer
Aug. 2012
Hippocratic Oath – 4th Century BC

- A statement on how we, as Physicians, should conduct ourselves in our interactions with patients, colleagues, and the Health Care Community

- Daily vigil throughout our career as a Physician

- Greatness measured not by the diseases we treat or cure, but by how we interact with our patients & their families while we are treating those diseases.
Hippocratic Oath

- Obligation to interact ethically
  Willingness to do the right thing even when not in our self interest

  Trustworthiness: Truthfulness, Integrity, Promise-keeping
  Respect: Confidentiality, Dignity, Courtesy
  Caring: Love, Benevolence, Altruism
  Responsibility: Accountability, Perseverance, Self-restraint
  Fairness: Equality, Impartiality, Tolerance & Acceptance
  Citizenship: Civility, Community

- These concepts are embraced in the UC Code of Conduct and the UC San Diego Health System “core values”
Outline

- UC Code of Conduct
  - 12 standards: ethical and business principles
  - How to report concerns
  - Safe & non-retaliation environment
- UC Health Care Vendor Relations
- HIPAA Privacy & Security
- Professional Conduct
- Questions & Resources
Introduction

- Members of the University of California community share a commitment to the highest ethical, legal, and professional standards in furtherance of our mission of patient care, teaching, research and public service.

- We recognize that we hold the University in trust for the people of the State of California.
Applicability

- The UC Code of Conduct (“Code”) applies to everyone who is a “member” of UC Health Sciences workforce including: faculty, medical staff, house staff, medical students, employees & volunteers.

- This Code is intended to provide guidance and be complimentary to the specific policies, procedures, ByLaws and rules enacted by the UC San Diego Health System.
1. Ethical Principles
2. Responsibility
3. Respect for Others
4. Privacy
5. Quality of Care
6. Medical Necessity
7. Accurate Financial Records
8. Conflict of Interest
9. Clinical Trials & Research
10. Accurate Clinical Records
11. Compliance with Laws & Policies
12. Government Investigations

Download a copy of the “Code of Conduct” from the UCSD Health Science Compliance Program, web-site: http://health.ucsd.edu/compliance
Professional Conduct – 911 !!

© Original Artist

Dr. Gregory House
Standard #1
Ethical Principles

- We adhere to the highest standards
  - We shall, at all times, conduct ourselves in accordance with the highest ethical, legal and professional standards.
  - We endeavor to hire the best, most qualified individuals and strive to attract, train and retain a diverse workforce.
Standard #2
Responsibility

- We take individual responsibility & accountability for our actions
  - We become familiar with the policies and laws that apply to our position and duties.
  - We comply with both their letter and spirit

- We ask questions!
  - Concerns about the appropriateness of any action (or failure to take action) should be reported:
    - Supervisor, Risk Management, Compliance Office, Internal Audit, or UC General Counsel.
    - Alternatively, you may call the UC Hot Line (1-800-403-4744). Callers may remain anonymous.
Standard #3
Respect for Others

- **We treat everyone with respect and dignity**
  - We make no distinction in the availability of services; or in the care we provide based on age, gender, disability, race, color, religion, or national origin.
  - We are committed to the compassionate treatment of patients and the respect of patient rights.
  - We act as positive role models and show due respect to subordinates and each other.
Standard #4  Privacy

- We manage health information, including EHRs / billing records, with CONFIDENTIALITY.
  - We access or use confidential information only to perform our job.
  - We do not share information with others unless they have a legitimate “need to know”.
  - We do not share passwords or post sensitive information or patient photos on unsecured web-sites or social media sites (e.g., Facebook, Twitter, YouTube…).

Reminder: Electronic activity is monitored for appropriate user access. Violations (including snooping) are subject to disciplinary actions…and personal fines.
Standard #5
Quality of Care

- We strive to attain the highest quality of patient care.
  - We provide quality health care in a manner that is safe, effective and efficient.
  - We place the interests of our patients above our own.
Standard #6
Medical Necessity

- We only provide care which is medically necessary.
  - We only order or render those services or items that meet objective criteria of medical necessity.
  - Patients may request a service that is not a covered benefit or medically necessary. The services may be provided as long as the patient has been given advance notice that a service is not a covered benefit and has agreed to pay for the services.
Standard #7
Accurate Financial Records

- We ensure that billing & financial records are accurate & complete
  - We only submit claims for payment to any payor for services that are medically necessary, actually performed, and have appropriate supporting documentation.
Standard #8
Conflict of Interest

- We avoid conflicts of interest and/or conflicts of commitment in our practices.
  - We do not give or accept gifts, gratuities, loans or other special treatment of value from third parties doing business with (or wishing to do business with) UC.
  - We do not contract for goods or services with family members of UCSDHS personnel.
  - We do not use UC funds to contribute to a political party, committee, organization or candidate in connection with a public campaign.
  - We avoid relationships which have the potential to unduly influence our clinical decision making.
  - We report actual / potential conflicts of interest / commitment. [http://coi.ucsd.edu](http://coi.ucsd.edu)
Standard #9
Clinical Trials & Research

- We conduct clinical trials & research consistent with ethical principles and all applicable UC policies, State and Federal laws, and regulatory requirements.
  - We protect the rights of study participants, including privacy rights.
  - We conform to the highest standards of research integrity.
  - We avoid plagiarism, misrepresentation, and falsification of data.
  - We conduct research in strict conformity with human research protection procedures. [http://irb.ucsd.edu](http://irb.ucsd.edu)
Standard #10
Accurate Clinical Records

- We create, maintain, and preserve patient records and documentation conforming to all applicable legal requirements, professional standards, and UC policies.
  - We do not knowingly create records that contain any false, fraudulent, fictitious, deceptive or misleading information.
  - We do not delete any entry from a medical record.
    - Records may be amended to ensure accuracy. Amended records must include the date, time, reason, and authentication.
  - We do not sign someone else’s signature unless clearly marked that we are signing on behalf of another (e.g., by initialing the signature).
  - We do not destroy, obliterate or remove any University records from the University’s premises.
Standard #11
Compliance with Laws & Policies

- We comply with all University policies, State & Federal laws, and regulatory requirements in dealing with patients, payers, vendors, health care providers, and business associates.
  - We do not accept or offer for individual benefit anything of value in exchange for the referral of patients or business.
  - We adhere to anti-trust laws prohibiting actions such as price-fixing, or improper sharing of competitive information.
  - We ensure that goods and services are procured in a competitive and fair manner.
We co-operate with authorized governmental investigations and audits.

- We have the right to consult a supervisor, Compliance Officer, Risk Manager or UC General Counsel before answering questions.
- We do not destroy documents.
- We do not lie or make misleading statements.
Reporting Violations


○ Alternatively, you may make a report anonymously:
  - Call the UC Hot Line, open 24 hrs, 1-800-403-4744.
  - The University will make every reasonable effort to keep confidential the identity of anyone reporting a suspected violation.

Who to report concerns to:

• Direct supervisor
• Human Resources (HR)
• COO, CMO, CEO
• Compliance Officer
• Risk Management
• Internal Audit
• UC Legal Counsel

Non-Retaliation Policy

- University employees are prohibited from retaliating against an employee who has made a good-faith report or refused to obey an illegal order, even if the allegation ultimately proves to be without merit.

- UC will, however, pursue disciplinary actions against any member who is shown to have knowingly filed a false report.

- UC Whistleblower Policy: http://ucwhistleblower.ucop.edu
Enforcement

- **Code of Conduct will be enforced!**
  - All UCSD workforce members are **expected** to report suspected code of conduct violations.
  - Managers & supervisors are **required** to report allegations & suspected violations.
  - Everyone is expected to cooperate fully with any investigation undertaken.
  - Corrective & disciplinary actions will be applied in response to violations consistent with UC policies.
  - UC may make appropriate disclosures to governmental agencies.
Intent:
- To guide & govern the appropriateness of interactions between physicians and the health care vendor industry.

Purpose:
- To prevent the perception, and reality of vendors unduly influencing clinical decision making.

Reason:
- Evidence based literature (Brennan, JAMA 2006; 295(4):429-433)
- AMC national trend
- Government scrutiny; Federal Sunshine Disclosure Laws
# UC Health Care Vendor Relations Policy

<table>
<thead>
<tr>
<th></th>
<th>Vendor Access</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>By prior appointment only</td>
<td>Confined to non-patient care areas</td>
</tr>
<tr>
<td></td>
<td>Registered: <a href="http://www.RepTrax.com">www.RepTrax.com</a></td>
<td>UCSD vendor ID badge required</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Gifts</strong></td>
<td><strong>Prohibited.</strong> Vendors may not provide free items (including food, beverages, pens, etc.) directly to UCSD employees and trainees.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Promotional Items</strong></td>
<td>Branded health care industry promotional items are prohibited in all UCSDHS sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Patient education materials: Permitted, but must be free of bias.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Samples</strong></td>
<td>Samples for personal use are prohibited.</td>
</tr>
</tbody>
</table>
Privacy Laws: HIPAA, HITECH, CMIA…

- **Federal laws**: “Health Information Portability & Accountability Act”; “HITECH Act”; “Red Flags”
  - Purpose: To ensure the public that health information is protected and to provide patients with privacy rights.
  - PHI = “Protected Health Information”

- **State laws**: AB-1298, “Identity theft notification”; AB211 / SB541: “Unauthorized access notification”
  - Purpose: Expands HIPAA to ensure that personal information is protected and that consumers are notified of breaches – including unauthorized access (snooping).
  - PII = “Personally Identified Information” – includes medical & health insurance information
  - Fines can be assessed to institutions and **individuals!**
    - Other risks: Notice to the medical board; further litigation
HIPAA Privacy & Security

- Patients expect physicians to protect their confidentiality & right to privacy
- Physicians should protect their patient’s confidentiality
- HIPAA requires physicians to protect their patient’s confidentiality
  - Violations require disciplinary actions up to and including terminations
  - Breaches of medical information require disclosure to the patient
  - Criminal, civil actions & fines are realistic possibilities
HIPAA: 3 Rules to Remember

- **Rule #1**: Access, use or disclose a patient’s PHI (protected health information) *only* if you have a “need to know”.

- **TPO test:**
  - **Treatment**: Are you a member of the patient’s care team?
  - **Payment**: Are you responsible for coding & billing activities?
  - **Operations**: Are you involved with QA/patient safety, teaching?

- Access, use or disclosure of PHI is also permitted:
  - With the patient’s prior written “HIPAA-valid” authorization
  - Or without authorization -- if the disclosure is required by law, e.g., child / elder abuse
HIPAA: 3 Rules to Remember

- **Rule #2**: Access, use, or disclose only the “minimum necessary” information.

- **Self-Test:**
  - Do you need the information to do your job?
  - What is the minimum information needed?
  - Is it reasonable to de-identify the data prior to storing or further permitted disclosures?
  - Are you storing / transmitting identified information in a secure manner?
    - If the information cannot be de-identified and if it is stored on mobile devices (i.e., laptops, USBs, ipads), or sent via e-mail attachment (outside of UCSD), **it must be encrypted (125+)**.


Rule #3: Maintain the security of electronic data (ePHI)

**Always:**
- Log-on with your own user ID & **strong** password
- Log-off or lock your session & lock-up laptops (out of sight)
- Delete unneeded ePHI/PII electronic data & e-mail files
- Encrypt ePHI if it must be stored on portable media

**Never:**
- Share your password
- Store restricted data on laptops, C-drives, or flash drives unless there is a UC business purpose **and** the **data** is **encrypted**.
- Identify a patient’s SSN in an e-mail or e-mail subject line
DO NOT SNOOP OUT OF CURIOSITY

- HHS Office of Civil Rights (OCR) investigates privacy complaints
- User access to patient information leaves an electronic “footprint” and is proactively monitored.
- Unauthorized access, use, viewing or disclosure of PHI is against State & Federal privacy laws
- Violations WILL result in corrective & disciplinary actions
- Breaches are reported to regulatory authorities and to the patient. Licensed facilities must report within 5 business days!
- Breaches may result in personal fines, reports to the medical board and in certain cases, require public disclosure.
HIPAA & California Laws: Problem Data Identifiers

- **It’s bigger than you think** -- anything with full name + SSN, DL#, CCNs or financial account data, or medical / health insurance information is protected by California law.

- **Examples:**
  - Payroll, visa / passport copies, W-2
  - Applications and resumes
  - Injury / doctor reports
  - Health benefit forms
  - Personal & family information
  - Reimbursement forms & financial records
  - Patient lists, case reports

Avoid storing unencrypted PII:
- Person’s full name plus any one of these identifiers…
  - DL# = Driver’s license
  - SSN# = Social Security#
  - CCN = Credit card #
  - MRN = Medical record #
  - Medical information
  - Health Insurance Information
HIPAA: Data Security Safeguards

- Don’t have it
- De-identify it
- Delete it
- Encrypt it (128+) ... and email attachments with PHI

- Notify the Privacy Office immediately if you lose it! (619-471-9150 or eQVR:confidentiality)
Encryption: Learn how to…
http://webhipaa.ucsd.edu

- Microsoft Office 2003: files encrypted at the file level:
  - Choose: File, Save as, advanced,
  - Choose: RC4 - [AES] and 128 bit

- Microsoft Office 2010, select “Prepare” from the MS button
- WinZip Pro + encrypt (AES256) + use a strong password!

- Other options: Consult with your system administrator regarding encryption products such as:
  - PointSec or Credant which offer master password safeguards; or TrueCrypt software (free); or File Vault for Mac; or
  - Flashdrives with encryption, e.g., LexarSecure-II USB drive and be sure to create a password protected “encrypted vault” on the drive.
  - Encrypt data before using any “Cloud” services… check before using cloud services for UCSD’s data, ask for help

Note: Password protected data is **not** the same as Encryption!
Usage of Social Networking Sites: Blogs, Twitter, Social Networking Sites, YouTube, Facebook...

- Be responsible, **avoid** unprofessional practices:
  - Do not share “PHI” or post anything about patients (identified or not)
  - Do not post photos of patients
  - Avoid “friending” (or being “friended”) by patients on personal sites
  - Avoid looking for patient profiles on social media sites
  - Do not post “skits” on YouTube which identifies patients or UCSD
  - Do not post unprofessional comments or “blogs” that may embarrass you or others
  - Do not use patient identifiers in power-point files in public forums/web

- General guidelines:
  - Take extreme care with privacy settings.
  - Be aware that your Facebook behavior may be observed by patients.
  - Never give medical advice via Facebook or other social sites.
  - Keep wall posts, tweets and other social communications within standard ethical practices of being a physician
Security Reminders

Password Required

Password protect computers, ipads & smartphones

Backup your electronic information

Protect software from malware: Install patches promptly for software programs that you install

Send e-mail securely

Empty e-trash: email; recycle bin; cookies; temp internet files

Encrypt restricted PII data on mobile devices & lock-up to prevent loss / thefts.

LOCK-UP

Run Anti-virus & Anti-spam software, Anti-spyware

Be green: “Diskwipe” before recycling old computers / disks / USBs / smartphones…
UCSD Medical Group’s Principles of Professional Behavior

“Membership in the UCSD Medical Group is a privilege and members are expected to hold themselves and each other to the highest standards of professionalism, ethics, personal conduct and citizenship.

These standards apply to all interactions with patients, staff, colleagues, administration and the general public.

It is expected that medical care will always be patient centered and conducted in a manner that puts patient interests first.”
Questions?

- Kathleen Naughton
  Chief Compliance / Privacy Officer, UCSD Health Sciences
  Tel: 619-471-9152; E-mail: knaughton@ucsd.edu
  - Web: http://health.ucsd.edu/compliance/hipaa.shtml
  - UC Hot Line: 1-800-403-4744,
Resources

- UCSD Medical Center MCPs – intranet posting of policies/procedures
- UCSDHS Compliance / Privacy Program
  - [http://health.ucsd.edu/compliance](http://health.ucsd.edu/compliance)
  - Encryption education modules: [http://webhipaa.ucsd.edu](http://webhipaa.ucsd.edu)
- UCSD Campus Blink site
  - Campus policies (PPM 200-13) and COI guidance
  - [http://www.ucop.edu/ogc/coi/ucsd.htm](http://www.ucop.edu/ogc/coi/ucsd.htm)
  - Human Research Protection Program (HRPP/ IRB) [http://irb.ucsd.edu/](http://irb.ucsd.edu/)
  - UCSD Minimum Network Security Standards:
    - [http://blink.ucsd.edu/Blink/External/Topics/Policy/0,1162,16456,00.html](http://blink.ucsd.edu/Blink/External/Topics/Policy/0,1162,16456,00.html)
- University of California
  - Ethics & Conflict of Interest Policies
    - [http://www.universityofcalifornia.edu/compliance/ethics/](http://www.universityofcalifornia.edu/compliance/ethics/)
    - [http://www.ucop.edu/ogc/policies.html](http://www.ucop.edu/ogc/policies.html)
  - Health Care Vendor Policy:
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 / student number: _____________ <if known>
- Non-UCSD workforce member ID: ______________
  - Indicate your date of birth and last 4 digits of your last name.
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: ______________