4th Year Medical Student Courses

Dear Student,

Thank you for your interest in our pediatric elective program at Children’s Hospital Los Angeles (CHLA), an affiliate of the Keck School of Medicine of the University of Southern California. We offer such positions for those students who have completed an introductory clerkship in pediatrics (at least 3 weeks of inpatient & 3 weeks of outpatient experience). We do not, however, accept students more than 6 months in advance of their clerkship.

There are rotations in pediatric subspecialties. Our programs are for four (4) weeks only. All subspecialty electives (with the exceptions of Emergency Medicine and the Ward electives) are of a consultative type. Upon your acceptance in our program you will find the work essentially the same as that offered our senior students. You are expected to take histories, do physical examinations, follow patients both on the wards and in the clinics, attend lectures and seminars held here; you are a junior member of the patient care team.

These are elective rotations and carry no stipends, lodgings, meals, or pagers. According to the rules of the University of Southern California with whom we are affiliated, we are unable to make any final commitment more than 60 days in advance of an elective. Although we may offer a position up to six months in advance, the final confirmation will be mailed to you 60 days prior to your arrival. We offer either eight (8) weeks of electives or two (2) rotations.

CHLA accepts students from all LCME and COCA schools. We also provide clinical rotation opportunities for a limited number of visiting international students from our affiliated institutions, LCME accredited Canadian Institutions, and select GHLO participating institutions. To find out if your school is accepted, please visit http://www.keck.usc.edu/education/md-program/student-affairs/visiting-student-clerkships/international-applicants/.

Enclosed is an application for you to return to our office.

If you have any further questions, please feel free to contact Derek Halet at dhalet@chla.usc.edu or (323) 361-2127.

Office of Educational Affairs
Children’s Hospital Los Angeles
Step 1: Please Complete the Application below, Print, and Sign where indicated.

Step 2: Please Complete the AAMC Standardized Immunization Form (if you have not done so already).

Step 3: Upload the Completed Application and Immunization Form into VSAS.

STUDENT INFORMATION

Important: please Type Information prior to printing for signatures.

<table>
<thead>
<tr>
<th>Student Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email:</td>
<td>Phone:</td>
</tr>
<tr>
<td>Name of Affiliated Institution:</td>
<td></td>
</tr>
<tr>
<td>Date of Current PPD:</td>
<td>Date of Flu Vaccination:</td>
</tr>
</tbody>
</table>

Must be noted. Must be noted.
ADDENDUM B

CHILDRENS HOSPITAL LOS ANGELES

IMMUNIZATION SCREENING STATEMENT

I have received the vaccinations for the following diseases, or had these diseases:

☐ Measles
☐ Mumps
☐ Rubella (German measles)

TUBERCULOSIS SCREENING STATEMENT

I have received a Mantoux (PPD) or chest film, if appropriate, within the past twelve (12) months with the following results:

☐ The results were negative for tuberculosis.

☐ The results were a new positive for tuberculosis and I am currently being treated for tuberculosis and have been evaluated by a physician and followed that physician’s recommendations.

☐ The results were a new positive for tuberculosis, but I do not have an active case of tuberculosis.

☐ I did not have repeat skin testing since I have been positive by Mantoux (PPD) in the past and have been evaluated by a physician and followed that physician’s recommendations.

I declare that the information on this form is true and without omission to the best of my knowledge.

Practitioner Signature

Date
ADDENDUM C

CONFIDENTIALITY STATEMENT

In order to protect the confidentiality of patient care and hospital matters, Children’s Hospital Los Angeles considers all information regarding its patients, their families, hospital employees and hospital business as confidential. All board members, officers, employees, volunteers, residents/fellows, students, Medical Staff members or practitioners with temporary privileges are required to adhere to this policy and not release or disclose any information without appropriate written authorization. The hospital complies with all applicable federal (HIPAA) and state law regarding the release of protected health information.

This policy includes the confidentiality of medical staff records and procedures, all patient information, employee personnel files and information contained in the hospital computer systems.

Board members, officers, employees, volunteers, residents/fellows, students, Medical Staff members or practitioners with temporary privileges are also asked to refrain from discussing any patient information or hospital business in public areas, including corridors, elevators, the cafeteria, McDonalds, hospital lobbies or waiting rooms.

ACKNOWLEDGEMENT:

I have read and agree to comply with the Children’s Hospital Los Angeles, Confidentiality Policy. I understand that I am prohibited from divulging any information regarding patients, their families, employees or matters related to hospital business except as mandated by hospital policy and/or law.

Practitioner Signature Date
ADDENDUM D

CHILDREN’S HOSPITAL LOS ANGELES
Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
Effective April 14, 2003

Primary Goals of the HIPAA Legislation
- Assure health insurance portability
- Reduce healthcare fraud and abuse
- Simplify electronic administrative processes
- Guarantee security and privacy of health information

HIPAA is the most sweeping legislation to affect healthcare since Medicare in 1965. Nearly everyone will be affected: payors, employers, providers, clearinghouses, practice management system vendors, billing agents, and service organizations. In regard to protecting patient information, security is defined as the protection of information, data and systems from accidental or intentional access by unauthorized users. Common threats to patient information security include talking about patients, using identifiable information such as names, diagnosis, etc., in public areas.

Examples of Protected Health Information:
- Clinical information
- Name/social security numbers
- Name of relatives/family name/employer
- Health plan numbers/account numbers
- Telephone numbers/fax numbers/e-mails
- All dates related to the individual—birth, service
- Geographic subdivision smaller than state
- Any information that can reasonably identify a patient

Penalties for Non-compliance with HIPAA Regulations

<table>
<thead>
<tr>
<th>Monetary Penalty</th>
<th>Term of Imprisonment</th>
<th>Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td>$100</td>
<td>N/A</td>
<td>Single violation of a provision</td>
</tr>
<tr>
<td>Up to $25,000</td>
<td>N/A</td>
<td>Multiple violations of an identical requirement for prohibition made during a calendar year</td>
</tr>
<tr>
<td>Up to $50,000</td>
<td>Up to one-year</td>
<td>disclosure of individually identifiable health wrongful information</td>
</tr>
<tr>
<td>Up to $100,000</td>
<td>Up to five years</td>
<td>Wrongful disclosure of individually identifiable health information committed under false pretenses</td>
</tr>
<tr>
<td>Up to $250,000</td>
<td>Up to ten years</td>
<td>Wrongful disclosure of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm.</td>
</tr>
</tbody>
</table>

Failure to implement transaction sets can result in fines of $225,000 per year or more ($25,000 per requirement, times nine transactions). Failure to implement privacy and security measures can result in imprisonment.

Patient Rights

PAGE 5
• **Patients have the right to:**
  o Look at and obtain a copy of their health information
  o Know how their health information has been used and to whom it has been disclosed
  o File a formal compliant if their privacy has been violated
  o Patient or parental consent must be obtained before a patient’s health information can be released to family members
  o Protecting patient information includes all forms of communication – electronic, written and verbal

• **Notice of Privacy Practices**
  o Covered Entities must provide a simple explanation of their privacy practices. Direct treatment providers must make a good faith effort to obtain written acknowledgment of receipt of the notice of privacy practices.

• **Authorization**
  o All Covered Entities must obtain individual authorization for each use or disclosure of treatment, payment or health care operations (PHI) for non-TPO activities.

• **Minimum Necessary**
  o Employees should use only the information minimally necessary to do their job.

• **Business Associates**
  o Covered Entities may disclose PHI to business associates. They are required to have contracts that require their Business Associates to observe certain privacy standards listed in the Regulations.

• **Personal Representatives (Parents)**
  o HIPAA gives control of a minor's PHI to the parent, guardian, or person acting in loco parentis with certain exceptions.
  o HIPAA does not overturn state laws that give providers discretion to disclose PHI to parents or prohibit the disclosure of PHI to a parent.
  o Verification of the personal representative’s identity is a critical overlap with physical security.

• **Health-related Communications and Marketing**
  o Marketing activities using PHI require authorization from each person for each use of their PHI.

• **Research**
  o PHI may not be used or disclosed for research without the standard written HIPAA authorization or a waiver of authorization approved by the Committee on Clinical Investigations.
PRIVACY DO’S

- Immediately remove all patient health information from printers, fax machines and photocopiers.
- Dispose of protected health information in the appropriate confidential bin.
- When conducting a conversation regarding a patient, do so in a private place or speak quietly so you can’t be overheard.
- Keep medical records and other documents containing personal health information out of public view.
- When possible, close patient/examining room doors or draw curtains and speak softly when discussing patients’ health information.
- Treat other people’s confidential information as if it were your own.
- Password protect your laptop computer and your personal digital assistant (pda).
- Report privacy violations in the Hospital to the Privacy Officer, at Extension 1-2302, so we can improve our organization’s privacy practices.

PRIVACY DON’TS

- Don’t share confidential patient information with anyone who doesn’t need to know it to do his or her job.
- Don’t share passwords on your computer.
- Never access information about a patient unless you need it to do your job.
- Don’t walk away from open medical records, lab results, or computers etc. Close records first and use a bookmark, if necessary.
HIPAA COMPETENCY TEST

Instructions: Mark the correct answer.

1. Which of the following statements about confidentiality and protecting patient information are true?
   - [ ] Only authorized people are allowed to look at or use patient information
   - [ ] Any health information that can identify a person must be treated as confidential
   - [ ] Confidential information should be shared only with those who have the “need to know”
   - [ ] All of the above

2. In regards to protecting patient information, security is defined as:
   - [ ] The requirement that all patient information either be under lock and key or protected by security officers
   - [ ] The protection of information, data and systems from accidental or intentional access by unauthorized users
   - [ ] None of the above
   - [ ] All of the above

3. Which of the following standards require health care organizations to protect patient information?
   - [ ] Chain of Trust (COT)
   - [ ] Prospective Payment System (PPS)
   - [ ] Health Insurance Portability and Accountability Act (HIPAA)
   - [ ] Outcomes Assessment Information Set (OASIS)

4. Organizations that violate patient privacy and security standards can suffer penalties such as:
   - [ ] Fines, possibly in the thousands of dollars
   - [ ] Imprisonment
   - [ ] Bad public relations
   - [ ] All of the above

5. Common threats to patient information security include:
   - [ ] Talking about patients, using identifiable information such as names, diagnosis, etc., in public areas
   - [ ] Failing to log off the computer when finished
   - [ ] Maintaining patient listings and other information out of the view of unauthorized people
   - [ ] All of the above

6. Patients have the right to:
   - [ ] Look at and obtain a copy of their health information
   - [ ] Know how their health information has been used and to whom it has been disclosed
   - [ ] File a formal complaint if their privacy has been violated
   - [ ] All of the above

7. Protected health information (PHI) is any information that can identify a patient.
   - [ ] True
   - [ ] False
8. Talking about a patient’s condition or diagnosis, while in a public area, would be a violation of patient privacy even if the patient’s name were not mentioned.
   □ True
   □ False

9. Patient or parental consent must be obtained before a patient’s health information can be released to family members.
   □ True
   □ False

10. Protecting patient information includes all forms of communication – electronic, written and verbal.
    □ True
    □ False

Practitioner Signature                      Date
## ADDENDUM E
Practitioner Role in Environment of Care Codes (Overhead Paged)

### Call Ext. 33 for the following emergency codes
- Code Blue - Medical Team Emergency
- Code Green - Hazardous Spill
- Code Yellow - Trauma Team Activation
- Code Red – Fire Emergency
- Code Orange - Disaster Plan Activation
- Code 10 – Missing Patient that is not suspected of being abducted
- Code 12 – Bomb Threat
- Code 13 – Community Disturbance / Code Orange Stand-By
- Code 99 – Hospital Lockdown/ Patient Abduction

### Call Ext. 711 for Workplace Violence Codes
- Dr/Mr. Strong – Violent/Threatening Behavior Dr./Mr. Adam Strong – Armed Individual

### Identification Badges
- Your ID badge must be worn on the upper body with the photo facing forward at all times when on the premises.
- If you lose your ID, you must report it missing to Security (Ext. 12313) and the Parking Office (Ext. 12214).

### Visitor Badges
- All visitors (whether parents, guardians, families, vendors, etc.) must have a visible Visitor Badge on their person.
- Visitor badges are as follows:
  - Yellow Badge – inpatient care areas
  - Orange Badge – outpatient clinics
  - and labs Red Badge – Emergency Department
  - Blue Badge – Other Business
  - White Badge – limited access – 1st floor Anderson Building only

### Wrong Badge or No Badge
- All Medical Staff, House Staff, and pre- & post-doctoral fellows and employees are responsible for:
  - Escorting visitors without badges to the Guest Services Desk at the main entrance, or calling Security.
  - Asking if you can assist a visitor with the wrong badge who is in the wrong area. Example: Visitor with a blue badge is seen in an inpatient care area.

### Fire/Life Safety
- Rescue endangered patients/close doors
- Activate the alarm system
- Call Ext. 33 to report fire
- Contain the fire
- Extinguish the fire
- Know where the fire alarm and fire extinguishers are located
- Know that the hospital is a series of smoke compartments designed to prevent the spread of smoke and fire
- Know that you may be needed to help transfer patients to another area

### In Case of Fife – SAFE
- Safety of Life – Remove occupant & close door
- Alarm – Activate a manual pull station & dial 33
- Fight the fire – If safe to do so. Use extinguisher.
- Evacuate – if danger of smoke or fire spread

### Fire Extinguisher Use - PASS
- Pull the pin
- Aim the hose/extinguisher
- Squeeze the handle
- Sweep from side to side

### Evacuation Procedure
- Move horizontally beyond next fire/smoke door
- Move vertically, two floors minimum or unit capable of receiving patient type
- Meet at designated assembly area
- Account for all staff and patients
- Notify emergency operations center Ext. 12342
- of status/missing persons
- Patient Priority – those closest to danger, ambulatory, those you can move yourself, those you need help to move

### Emergency Preparedness/Disaster Procedure
- Code Orange will be announced overhead
- All available physicians report to the Personnel Pool located 1st floor Page 1-7A

### Medical Equipment Malfunction
- Remove from service and sequester any medical equipment you suspect or know was involved in a patient incident
- notify Risk Management immediately
- Assure that all equipment is reviewed by the Biomedical Dept. before it is used in patient care.
### Safety
- Know location of the Safety Manual
- Know to complete a Patient/Visitor Event Report in the event something unusual happens to you or your patient

### Hazardous Materials/Waste
- Wear proper protective gear
- Inquire regarding proper disposal of chemicals
- Require labels on all chemicals that are used by you
- Know where the MSDS for chemicals in your area are located

### Utilities Failure
- Know that the hospital’s emergency power generators will start in less than 10 seconds.
- Know that these power supply systems are tested on a weekly basis.
- You may be needed to assist patients whose equipment has failed
- Know processes to follow in event of utilization failure

### Infection Control
- Perform hand hygiene prior to every patient room entry and exit, between patient contact, before donning and after removing gloves, before handling an invasive device, after contact with body fluids or excretions, mucous membranes, non-intact skin or wound dressings and any time as needed such as after sneezing or coughing, and before handling food or oral medications
- Follow all posted instructions for wearing personal protective equipment
- Consult with any questions (Ext. 15510)

---

I have been oriented to the following information in Addendum E, Practitioner Role in Environment of Care:

- Codes
- Security Badges
- Visitor Badges
- Wrong Badge or No Badge
- Safety Management
- Hazardous Materials/Waste Management
- Fire/Life Safety Management
- SAFE – In Case of Fire
- Fire Extinguisher Use – PASS
- Evacuation Procedure
- Emergency Preparedness Management
- Medical Equipment Management
- Utilities Management
- Infection Control

---

**Practitioner Signature**  
**Date**