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/.

Please attach this supplemental application to your VSAS documents.

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

Office of Medical Educational
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>
</tr>
</thead>
<tbody>
<tr>
<td>Email:</td>
</tr>
<tr>
<td>Name of Affiliated Institution:</td>
</tr>
<tr>
<td>Date of Current PPD:</td>
</tr>
<tr>
<td>Must be noted.</td>
</tr>
</tbody>
</table>
DATE:_____________________________________

NAME:____________________________________________

Instructions: Please fill out this screening statement and provide proof (documentation) of immunizations records.

I have received the vaccinations for the following diseases, or had these diseases:
☐ Measles
☐ Mumps
☐ Rubella (German measles)
☐ TDAP (within the last 5 years)

**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.

________________________________________________________________________  ____________
Signature                                           Date

________________________________________________________________________
Print Name
Primary Goals of the HIPAA/HITECH Legislation

- Ensure health insurance portability
- Prevent fraud, waste, and abuse
- Simplify electronic administrative processes
- Establish standards to protect the privacy of health information

All Covered Entities (CEs) and their workforce members are required to abide by HIPAA/HITECH. “Covered Entities” include health plans, health care clearinghouses, and health care providers. The Act defines a “health care provider” as “a provider of medical or health services…and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.” The provider definition is very broad and includes non-traditional services, such as acupuncture and case management.

HITECH expanded the reach of HIPAA by applying the standards and requirements of the Act to Business Associates. In general, a Business Associate (BA) is any individual or entity that creates, receives, maintains, or transmits PHI on behalf of a Covered Entity for a regulated function or activity, such as claims processing, data analysis, quality assurance, etc.

**HIPAA Privacy Rule**

The HIPAA Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information” (PHI).

“Individually identifiable health information” is information, including demographic data, that relates to (1) the individual’s past, present, or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) the past, present, or future payment for the provision of health care to the individual, and identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers, including but not limited to:

- Name
- Mailing address, email address, telephone number, and fax number
- All dates related to the individual (date of birth, date of death, etc.)
- Social Security Number
- Medical Record Number
Effective Date: 4/3/17

- Biometric identifiers (finger and voice prints)
- Full face photographs and other comparable images

**Penalties for Non-compliance with HIPAA/HITECH Regulations**

Individuals who fail to comply with this policy will be subject to sanctions under *ADM 096.0 Sanctioning of Workforce and Mitigation* and *ADM 049.0 Disciplinary Counseling Procedures*, up to and including termination, in addition to monetary fines and possible imprisonment under federal law.

**Patient Rights**

- Access
  - Right to access and receive a copy of one’s own PHI (in paper or electronic format)
- Amendment
  - Request an amendment to information believed to be incomplete or incorrect
- Accounting of Disclosures
  - Information about how the patient’s health information has been used and to whom it has been disclosed.
- Restriction
  - Right to request a restriction on the use and disclosure of the individual’s PHI (including a restriction on disclosure to a health plan for services paid-in-full by the individual)
- Confidential Communications
  - Right to request alternative forms of communications (e.g. mail sent to PO Box instead of street address, no messages on home answering machine, etc.)
- Complaints
  - Patients have the right to file a formal complaint, to the hospital and/or the Office for Civil Rights in the Department of Health & Human Services (OCR), the entity that oversees and enforces HIPAA/HITECH, if they believe their rights have been violated.
- Notice of Privacy Practices (NPP)
  - A covered entity must provide patients with a Notice of Privacy Practices (NPP), notifying individuals of the entity’s legal duties and privacy practices with respect to PHI.

**Authorization**

Unless otherwise authorized by law or CHLA policy, a patient/personal representative’s written consent must be obtained before his/her PHI may be used or disclosed for purposes other than treatment, payment, or operations.

Except in certain situations, uses and disclosures of PHI must comply with the principle of Minimum Necessary, which requires a covered entity or business associate to make reasonable efforts to use, disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request.

Prior to disclosing any PHI, the individual must verify the recipient’s identity and authority to receive the PHI. For example, the parent or legal guardian of a minor child is the patient’s “personal representative” and therefore able to receive information about his/her treatment, diagnosis, etc.

Any inappropriate viewing of a patient’s medical or financial information without a direct need for diagnosis, treatment, payment, or other lawful use is considered “unauthorized” and subject to the sanctions outlined
above. Under HIPAA, a breach is generally defined as any impermissible use or disclosure of health information under the Privacy Rule that compromises the privacy or security of the PHI.

**PRIVACY DO’S**

- Immediately remove all patient health information from printers, fax machines, and photocopiers.
- Dispose of protected health information in the appropriate confidential shredding 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 when discussing patients’ health information.
- Ensure that all devices used to access or store CHLA data and protected health information (PHI) are encrypted in compliance with applicable CHLA policies. This includes laptops, desktops, tablets, smartphones, etc.
- Report potential privacy violations to the Chief Compliance & Privacy Officer, at Extension 12302, or by email to privacy@chla.usc.edu.

**PRIVACY DON’TS**

- Don’t share confidential patient information with anyone who doesn’t need to know the information to perform his or her job function.
- Don’t share passwords or allow anyone else to use your login credentials.
- Do not leave devices used to store or access CHLA data unattended, including in a vehicle or unlocked office.

**HIPAA COMPETENCY TEST**

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. What kind of individually identifiable health information is protected by the HIPAA Privacy Rule?
   - Paper
   - Electronic
   - Verbal
   - All of the above

4. Organizations that violate patient privacy and security standards can suffer penalties such as:
   - Fines, possibly in the millions of dollars
   - Imprisonment
   - Negative publicity and reputational harm
   - 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 in public view
   - 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. What makes a strong password?
   - Using at least 8 characters
   - Using mixed upper and lower case characters
   - Using special characters or symbols
   - All of the above

8. You accidentally fax paperwork containing PHI to the wrong number. The recipient calls to let you know, and agrees to destroy the documents immediately. Should you report this to the Compliance Office?
   - Yes
   - No

9. Unless authorized by law or CHLA policy, a patient/personal representative’s written consent must be obtained before his/her PHI may be used or disclosed for purposes other than treatment, payment, or operations.
10. Any device used to access or store CHLA data must be encrypted.
   ☐ True
   ☐ False

I have read and understand all materials presented about HIPAA and HITECH.

_________________________________________  _________________________
Signature                                                Date

_________________________________________
Print Name
CONFIDENTIALITY STATEMENT
ADM – 067.3 Attachment C

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/HITECH) 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, the Interfaith Center, hospital lobbies or waiting rooms.

ACKNOWLEDGEMENT:

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

Signature________________________________________Date___________
## I. Call Ext. 33 for the following emergency codes
- Code Blue: Medical Team Emergency
- Code Orange: Hazardous Spill
- Code Yellow: Trauma Team Activation
- Code Red: Fire Emergency
- Code Pink: Infant Abduction
- Code Purple: Child Abduction
- Code Gray: Combative Person
- Code Silver: Person with weapon and/or active shooter and/or hostage situation
- Code Triage Internal: Activate Emergency Operations Plan for internal incident

## II. 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)

## III. 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

## IV. 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

## V. 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.

## VII. 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 FIRE – 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

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

## IX. 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

## X. Medical Equipment Malfunction
- Remove from service and sequester any medical equipment you suspect or know
- You may be needed to assist patients whose equipment has failed
- Know processes to follow in event of utilization failure

### VI. 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)

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.

---

I have read and understand information on the CHLA Environment of Care:

_________________________    ____________________
Signature                           Date

_________________________
Print Name