UCSF Benioff Children's Hospital Oakland

APPLICATION

4th year Medical Student Clerkship

Thank you for your interest in our Medical Student Clerkship Program.
We accept students who are currently in, or will be in their fourth (4th) year of medical school during the clerkship.

Last Name: _____ First Name: _____ M Initial:_____

Home Address: _____ City: _____ State:___ Zip:_____

Email: _____ Cell Phone:_____

Date of Birth: _____ Last **5 digits** of Social Security No:XXX-X - _____

Name of Medical School:_____

Expected Degree: ☐ M.D. or ☐ D.O. Expected Graduation date: _____

Are you applying to the Diversity Scholars Program (DSP)? Yes ☐ No ☐

Desired Dates of Rotation: _____
(Please give two date ranges in order of preference)

Desired rotation: _____
(Please state your top three choices in order of preference)

REQUIRED DOCUMENTATION:

The following list of required documentation must accompany this application and must be received no less than 6 weeks prior to start date of rotation*. Check off each, and include with your packet. You may email the entire packet to medstudent@mail.cho.org (Pdf only; do not send jpegs), or send by regular post; processing fee should come by regular post. Incomplete packets will be denied and returned.

- ☐ Letter of good standing
- ☐ Copy of Malpractice Certificate (Including amount of coverage and policy effective dates)
- ☐ Copy of your transcript
- ☐ Copy of all USMLE Step Score Reports
- ☐ Evaluation of 3rd year pediatric core rotation showing at least **2 weeks inpatient experience**
- ☐ Mask fit proof and results (must show date as less than one year)
- ☐ Immunizations: proof and dates required
  - ☐ MMR ☐ Hepatitis B ☐ Recent flu ☐ Tdap
  - ☐ PPD within the last 12 months _____ ☐ Varicella
  - ☐ PPD within 3 months of start of rotation _____
- ☐ *For ADOLESCENT MEDICINE Applications ONLY:

  Oakland Unified School District REQUIRES a Live Scan, and some additional documentation from your school for our school-based clinics. Applications for this rotation are due **4 months prior** to your proposed start date. Once your application is accepted, complete the Live Scan; proof must be dated and received by our office **90 days** prior to your proposed start date in order for you to be eligible for the rotation. Keep your receipt as you will be reimbursed for this cost when you arrive. We will send information for the documentation once the application is accepted.

☐ Privacy Confidentiality Form

☐ Photography and Publication Consent Form

☐ ***Processing Fee***: Include a check for $100 made out to "UCSF Benioff Children's Hospital Oakland".

PLEASE SEND DOCUMENTS IN ONE COMPLETE PACKET:

Attention: Katherine Castillo
Graduate Medical Education Department
UCSF Benioff Children's Hospital Oakland
747 52nd Street, Room 245
Oakland, CA 94609-1809

FOR OFFICE USE ONLY:

V 2.28.2018

Date received: _____ Reviewed: _____ Application complete: Y/N Fee rec'd: Y/N Missing documentation: _____
Last 5 of SS#: _____ Live Scan _____ or N/A 2nd PPD:_____ Approved: Y/N Letter sent: Y/N Date sent: _____

E07 PRIVACY, CONFIDENTIALITY & SECURITY OF INFORMATION

I. POLICY:

CHRCO values the privacy and confidentiality rights of patients, families, and proprietary Hospital information. All employees and affiliates of CHRCO who have access to such information are obligated to honor the laws and organizational values of privacy and confidentiality, and to protect and safeguard information against unauthorized use, disclosure, or corruption. Acknowledgement of, and agreement to, the policy is a condition of employment. To ensure confidentiality and security, employees and affiliates are not to access, alter, remove, copy, transmit, or otherwise convey information except to conduct legitimate hospital business. This policy addresses the privacy, confidentiality and security of all information, regardless of the medium in which it is viewed, stored, or maintained.

Laws controlling the privacy of, access to and maintenance of confidential information include, but are not limited to the:

- *Federal Health Insurance Portability and Accountability Act (HIPAA),*
- *California Information Practices Act (IPA),*
- *California Confidentiality of Medical Information Act (COMIA), and*
- *Lanterman-Petris-Short Act (LPS).*

These and other laws apply whether the information is held in electronic or any other form, and whether the information is used or disclosed orally or in writing.

Associated CHRCO policies that control the way confidential information may be used include, but are not limited to the following:

- *Hospital Information Systems "Information Security"*
- *Medical Records Department "Confidentiality"*
- *Medical Records Department " Release of Information"*
- *Medical Records Department "Security of the Medical Record"*
- *Administrative "Code of Conduct"*
- *Administrative "Internet Access"*

II. DEFINITIONS:

Affiliates of CHRCO include, but are not limited to:

- Physicians and their office staff
- Residents, interns, and students of medical or allied health programs
- Volunteers, temporary and on-call staff
- Business Associates, contractors and vendors
- Authorized medical plan reviewers and other individuals engaged in reviewing medical records

CHRCO records and files are the legal property of CHRCO and include:

- All medical information as defined in this policy
- Proprietary CHRCO information and databases
- Employee records and files
- All e-mail messages

Confidential information includes information that identifies or describes an individual and the disclosure of which would constitute an unwarranted invasion of personal privacy. Examples of

confidential employee and CHRCO business information include home address and telephone number; medical information; birth date; citizenship; social security number; spouse/partner/relative's names; income tax withholding data and performance evaluations and proprietary/trade secret information.

Individual accountability is the foundation upon which all confidentiality and security policies are based. While all reasonable means are taken to govern access to information, each employee or affiliate is ultimately responsible for any activity occurring through his/her user ID code, and in upholding the CHRCO policies.

Medical information includes the following: medical and psychiatric records, including paper printouts, photos, videotapes, diagnostic and therapeutic reports, x-rays, scans, laboratory and pathology samples; patient business records, such as bills for service or insurance information whether stored externally or on campus; electronically stored or transmitted patient information; visual observation of patients receiving medical care or accessing services; verbal information provide by or about a patient; peer review/risk management information and activities; or other information the disclosure of which would constitute an unwarranted invasion of privacy.

Minimum Necessary Standard is to be followed when accessing medical information. For example, although physicians, nurses and care providers may need to view the entire record, a billing clerk might only need to see a specific report to determine the billing codes. An admissions staff member may not need to see the medical record at all, only an order form with the admitting diagnosis and identification of the admitting physician. Only access and use the patient information that you need to do your own job.

Protected Health Information is defined under medical information. Its acronym, PHI is commonly used.

Violations regarding the use of hospital records, files or equipment will be subject to appropriate disciplinary action. Violations include, but are not limited to:

- Unlawful disclosure of information
- Removal of patient and hospital records from the premises without proper authorization
- Use of the CHRCO network for illegal, inappropriate, or obscene purposes, or in support of such activities
- Intentional disruption of network traffic or system crash
- Gaining or seeking to gain access to resources or entities for which an individual has no right to access
- Forging electronic mail messages or using an account owned by another
- Invasion of privacy
- Use of CHRCO equipment for commercial or financial gain or fraud.

III. CONFIDENTIALITY

1. All new hires are given a copy of this Privacy, Confidentiality and Security policy and must sign a hard copy agreement on the last page of the policy as part of the new hire paperwork. The agreement is maintained in the employee's Human Resources file.

2. When granted access to the CHRCO's computer system, the Confidentiality Agreement is displayed on-line and the user must acknowledge it as part of the condition of receiving a password. Every six months when a user's password automatically expires, the agreement must be re-acknowledged in order to receive another password to the system.

3. When participating in the De'Medici safety and security training, each participant again receives a reminder of security and confidentiality policies, and again must acknowledge the agreement.

IV. ACCESS

1. **Standard access:** Access to information is managed on a need-to-know basis, and applies to all patient, employee, or hospital information in both paper and electronic form.

   A. Information held in paper form such as business, employee and other medical records are to be
      1) stored in secure areas
      2) never left in locations where unauthorized users can access the information.
      3) When no longer needed, confidential information in paper form must be discarded using the confidential paper bins. Shredding may also be used as long as the information on the shredded paper is no longer identifiable.

   B. Password and access management policies have been established by the Hospital Information Systems Department for the use of electronic systems
      1) An administrator, authorized department supervisor, or their designee, must submit all password and access requests to the HIS Department through the on-line Order Entry Requisition routine.
      2) The HIS Department creates a user account in which access to specific applications is identified and appropriate access is assigned.
      3) The authorized requestor, in consultation with HIS, establishes the nature and extent of the access allowed for the user. Within each application, a menu consistent with the user's required level of access is identified from a file of customized menus, or if necessary, a unique menu is designed. Applications, databases, or routines not assigned to the user are completely inaccessible and do not display on the menu.

2. **Remote access:**
   A. A user's Administrative Conference member must authorize remote access.
   B. All the policies and procedures for standard access apply.
   C. Users who are granted remote access must exercise due diligence in protecting data and information found on the Hospital's system. The user is responsible for preventing access by those not expressly authorized, and must observe and comply with the Hospital's policies regarding confidentiality and security of information.
   D. Any unauthorized access, dissemination, or discussion of confidential information shall be reported immediately to Administration, resulting in appropriate disciplinary action.
   E. Community physicians requesting remote access for their office personnel are responsible for their staff's adherence to CHRCO's policies and procedures.
   F. Remote access logs are audited daily for proper log-on protocols and length of time on the system.

3. **Internet access**

   A. Internet access is provided as a service to selected desktop computers through an external Internet Service Provider.
   B. All employees will use the Internet only for business purposes related to research, education, and patient care. All other uses subject the employee to disciplinary action, up to and including, termination.
   C. Management will periodically audit the use of the Internet.
   D. See the Administrative Policy on Internet Access for the full policy and procedure relating to the use of the Internet.

V. RELEASE OF INFORMATION

1. When possible, all requests for medical information should be forwarded to the Medical Record/Health Information Department, where requests are logged with pertinent information and processed by trained personnel.

2. Patient information may be released only if an appropriate authorization is obtained prior to the release of information, or in the case of a medical emergency.

3. Test results of HIV and sexually transmitted diseases, mental health records, substance abuse records, and other sensitive information cannot be released without special authorization. Refer to trained staff in Medical Department for assistance.

4. Business information contained in Human Resources records, Financial systems and reports and/or other non-medical business information must be directed to the appropriate department for response. If unsure, a manager is to be consulted to insure the appropriate routing of the request for information.

VI. USE OF THE ELECTRONIC SYSTEM

1. Passwords may not be disclosed to another individual. Password sharing is considered disclosure of confidential information. Password disclosure includes, but is not limited to, allowing another to use your log-on, displaying passwords on badges or computers, and actively stating your password.

2. A user should sign off the system when work is completed to prevent disclosure of information to individuals not authorized to have such information. Menus automatically sign themselves off or "time out" after a period of no keyboard activity.

3. The computer system limits the number of sign-on tries to three times, after which the keyboard is locked for 60 seconds and logged as a security violation on the system audit logs.

4. An employee's department manager or affiliate's sponsor is responsible for ensuring that the employee has completed all training required for the access given and for ensuring that the employee/affiliate understands the confidential nature of the password, as well as the data to be accessed.

5. All terminated employees will have their password and access inactivated by HIS.

VII. USE OF FACSIMILE (FAX) MACHINES

1. As with all types of disclosure, patient information can be released via fax only with an appropriate authorization, unless a medical emergency (defined by a clinician) necessitates a release without an authorization. Releases should be coordinated through the Medical Records/Health Information Department. Refer to Medical Records policies on Release of Information via Fax.

2. A properly executed authorization transmitted via facsimile is acceptable.

3. Information should be limited to that necessary to meet the requestor's needs.

4. Information sent via fax must contain a cover page with the Hospital's confidentiality notice, indicating the privileged nature of the communication and the procedure to follow if the communication is received in error. The cover page statement is as follows:

   FAX COVER LETTER CONFIDENTIALITY STATEMENT
   The information in this facsimile (FAX) transmission is considered confidential and privileged, and is protected by law and is meant for the use of the intended recipient. Any dissemination, distribution or copying of this transmission or information is a violation of the law and is prohibited. If you received this transmission in error, please destroy all of it immediately and contact the sender. If you would like to request additional information about the faxed material, call the Hospital operator listed below and ask to speak to the individual whose name is listed in the "FROM" field above. To report problems of a technical nature, such as receiving multiple copies of the same fax or receiving incomplete information, contact the Hospital Information Systems Department at the number listed on the next page.

   CHRCO HOSPITAL OPERATOR: (510) 428-3000
   INFORMATION SYSTEMS: (510) 428-3636
   747 52 nd Street
   Oakland, CA 94609-1809 (Technical assistance only)

5. Because receipt of information at the recipient's end cannot be controlled or guaranteed, use of a fax machine for transmitting patient information should be used judiciously and not simply for the convenience of the requesting party. Routine disclosure of information to insurance companies, attorneys, or other legitimate users is discouraged.

6. Reasonable efforts should be made to assure the fax transmission is sent to the appropriate destination. Destination numbers should be preprogrammed into the machine, if possible, to eliminate errors in transmission from misdialing.

7. Managers are responsible for assuring that fax machines are located in secure locations in their area, and that access to them is limited. When possible, one or more individuals should be designated to monitor incoming documents and to remove them immediately, examine them to ensure receipt of all pages, and deliver them to the appropriate parties.

8. Facsimile machines throughout the organization bear the following label:

Facsimile Usage Agreement Statement
The use of this facsimile machine is for express and legitimate CHRCO business. Transmission f CHRCO patient, employee, financial or other related information is not allowed, unless authorized by Medical Records, Medical Staff or Senior Administration. The sender agrees to and is bound by CHRCO's Confidentiality of Information policy. Misuse of CHRCO facsimile machines to disseminate, distribute, or copy privileged and confidential information is not permitted and is a violation of the Confidentiality and Security of Information policy

VIII. USE OF E-MAIL

1. The same features that make e-mail a powerful communication tool also make it vulnerable to security breaches. Once an e-mail reaches its destination, the user loses control over it, as recipients can easily forward e-mails to someone else or store the messages in unsecured files. Therefore, all users must understand the risks in transmitting information via e-mail, and use caution in employing this technology.

2. Assume normal e-mail systems are not secure unless you have clear information that the system is encrypted or in other ways secure.

3. Be careful what you send via e-mail. Do not send confidential information unless you can de-identify it. Warn patients who communicate with you via email that their confidentiality cannot be ensured.

4. Use the same care in sending e-mails that you would with a letter. Do not write anything in an e-mail that you might regret later. E-mails are never erased.

5. Do not send attachments containing protected health information without encryption.

6. Add a confidential message footer to your messages, such as:
***CONFIDENTIALITY NOTICE** This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.*

IX. VOICE MAIL, ANSWERING MACHINES, TELEPHONE COMMUNICATION

1. Consider who has access to your voicemail or answering machine so others do not access PHI.

2. Take care what messages you leave on answering machines and voice mail.

3. If you use the speakerphone, be aware of your surroundings and sensitive to the messages being replayed.

X. MOBILE COMPUTING FOR DEVICES CONTAINING PHI

1. NEVER leave equipment in an exposed or unsecured area.

2. ALWAYS password-protect portable equipment such as laptops and personal data assistants (PDAs).

3. Frequently make protected backups of data stored on remote systems.

4. Never leave information or information systems containing PHI open to access, while unattended.

5. Telecommuters and others working at home should follow similar security and privacy protocols at their off-site and/or home offices.

6. Use caution when uploading or downloading files to/from PDAs. Adhere to the "minimum necessary" standard.

7. Off-site work requires greater vigilance to maintain the required level of privacy and security.

XI. AUDITING PROGRAM

1. The computer system maintains an audit trail of all information accessed. Audit trails include date and time of access, the individual who accessed the information, length of time the information was viewed, and what category of information was accessed.

2. Any manager who has identified a potential breach of confidentiality or security can request audits, and a hard copy audit trail can be obtained.

3. The Hospital Information Systems Department conducts daily or periodic audits of system access. They include:
   A. Remote access logs
   B. Acknowledgement of confidentiality agreements
   C. Audits of patients marked "confidential" or patients with "high-profile" cases.

XII. INACTIVATION OF PASSWORDS

1. The manager, Payroll, or Human Resources notifies HIS when a user terminates employment, and the user's account is then deleted.

2. The manager is responsible for notifying HIS immediately in the event of a problematic employee termination.

3. HIS can inactivate user accounts at any time if security of the system is potentially compromised. HIS will transfer a user's network and Meditech Magic Office files to the manager prior to deleting the account. Deletion will occur 30 days from notification or inactivation.

4. Payroll provides a list to HIS weekly so the inactivation of all terminated employee accounts can be verified.

XIII. DISCIPLINARY ACTION

1. Seeking, disclosing, or permitting others to disclose confidential information from the Hospital, unless specifically authorized, are prohibited acts and are grounds for disciplinary action.

2. Breaches of the policy may result in disciplinary action up to, and including, termination.

3. Managers and a Human Resources representative will determine the degree of disciplinary action to be taken. A member of Hospital Administration may also be engaged, if applicable.

4. Computer access codes and passwords are confidential, and their unauthorized use is prohibited. Sharing of passwords is considered disclosure of confidential information.

CHILDREN'S HOSPITAL
& RESEARCH CENTER OAKLAND

CONFIDENTIALITY AGREEMENT

Acknowledgement of Responsibility

I understand and acknowledge that:

It is my legal and ethical responsibility to preserve and protect the privacy, confidentiality and security of all medical records, proprietary and other confidential information relating to Children', its patients, activities and affiliates, in accordance with the law and organizational policy.

I agree to access, use or disclose confidential information only in the performance of my official duties, where required by or permitted by law, and only to persons who have the right to receive that information. When using or disclosing confidential information, I will use or disclose only the minimum information necessary.

I agree to discuss confidential information only in my workplace and for work-related purposes. I will not knowingly discuss any confidential information within the hearing of other persons who do not have the right to receive the information. I agree to protect the confidentiality of any medical, proprietary or other confidential information that is incidentally disclosed to me in the course of my relationship with Children's.

I understand that psychiatric records, drug abuse records, and any and all references to HIV testing, such as clinical tests, laboratory or otherwise, used to identify HIV, a component of HIV, or antibodies or antigens to HIV, are specially protected by law.

I understand that my access to all Children's electronic information systems is subject to audit in accordance with organizational policy.

I agree not to share my Login or User ID and/or password with anyone and that any access to Children's electronic information systems made using my Login or User ID and password is my responsibility. If I believe someone else has used my Login or User ID and/or password, I will immediately report the use to Information Technology Services and request a new password.

I understand that violation of any of Children's policies and procedures related to confidential information or of any state or federal laws or regulations governing a patient's right to privacy may subject me to legal and/or disciplinary action up to and including immediate termination from my employment/professional relationship with Children's.

I understand that I may be personally liable for harm resulting from my breach of this Agreement and that I may also be held criminally liable under the HIPAA privacy regulations for an intentional and/or malicious release of protected health information.

Signature: _____ Date: _____

ID Pin: _____

Print Name: _____ Department: _____

Consent for Photograph, Publish, Use, and/or Share Information

UCSF Benioff Children's Hospital Oakland

Medical Student Name_____ Date of birth_____

Today's date_____ This consent expires three (3) years from today.

I hereby give my consent to UCSF Benioff Children's Hospital Oakland ("Children's") and its affiliated organizations, including its fundraising foundation, to do any or all of the following with respect to me/my child:

1. **To take pictures, recordings, and/or information that may be used in and/or shared in the following sources:** Children's publications; print and/or online advertising; Children's websites[1]; Children's social media outlets (e.g.: Facebook, Twitter, YouTube, Instagram, Pinterest); Public media[2]
2. **To release:**
   ☐Medical information about me/my child ☐Interview with me/my child
   ☐Pictures or recordings of me/my child and/or ☐Artwork created by me/my child

I understand:

- I consent to Children's doing these activities in order to assist scientific, treatment, educational, public relations, marketing, news media, and fundraising goals. I and my successors, hereby hold Children's, its employees, physicians, and any other person participating in my/my child's care and their successors, harmless from the activities allowed by this agreement.
- I may request that the taking of Pictures/Recordings stop at any time.
- Pictures/Recordings/Information published online before the expiration date may remain online after the expiration date but will not be used in a new way without my consent.
- I may cancel this consent up until a reasonable time before the Pictures/Recordings/Information is used, but I must do so in writing and submit to: UCSF Benioff Children's Hospital Oakland, Marketing Department, 747 52nd Street, Oakland, CA 94609.
- My cancellation will be effective when received by Children's, except where use or sharing has already occurred in accordance with this consent.
- I may refuse to sign this consent. This will not affect my/my child's ability to get treatment or payment or eligibility for benefits.
- Information shared because of this consent could be re-shared by the recipient. Such re-sharing in some cases is not protected by California law and may no longer be protected by federal law.
- I will not receive any financial compensation for agreeing to this consent.
- I have a right to receive a copy of this consent.

Signature _____ Medical Student

Printed name _____ Relationship Self

Phone number _____ Email _____

Street address _____

City_____ State_____ Zip _____

Copy has been provided by: ☐Carbon Copy ☐Email ☐Postal

[1] Includes www.childrenshospitaloakland.org, www.give.ucsfbenioffchildrens.org, www.chori.org, www.100amazingyears.org.

[2] **Sharing information with Media:** Note that under California and Federal law, a provider may release certain basic non-medical information in limited circumstances even without this Consent. Please see the Children's Notice of Privacy Practices for additional information.

STAFF ONLY

Consent filled out by: Employee Name_____ **Dept**_____ ☐**Scanned**

Event_____ **Date** _____

Patient description (clothing, hair, etc.) _____

2016