AGENDA ITEM NO.
C-13

COUNTY OF HUMBOLDT

For the meeting of: December 8, 2015

Date: November 12, 2015

To: Board of Supervisors

From: Phillip R. Crandall, Director
Department of Health and Human Services

Subject: California Children's Services Electronic Records Access Agreement with UCSF Benioff Children's Hospital Oakland

RECOMMENDATION(S):
That the Board of Supervisors:

1. Approve the electronic medical records access agreement with UCSF Benioff Children's Hospital Oakland (CHO) for a term of three (3) years from the effective date.
2. Authorize the Chair to sign three (3) original agreements.
3. Authorize the Public Health Director or designee to sign future amendments to the agreement with CHO.
4. Direct the Clerk of the Board to return three (3) agreements to the DHHS-Contract Unit for forwarding to DHHS-Public Health Administration for execution by Contractor.

SOURCE OF FUNDING:
Public Health Fund

DISCUSSION:
California Children's Services (CCS) is a statewide program that authorizes diagnosis and treatment services and provides medical case management and physical and occupational therapy services to

Prepared by Anne Davis-Gervan AA II CAO Approval

REVIEW:
Auditor County Counsel Human Resources Other

TYPE OF ITEM:
X Consent
____ Departmental
____ Public Hearing
____ Other ____

PREVIOUS ACTION/REFERRAL:

Board Order No. ____

Meeting of: ____

BOARD OF SUPERVISORS, COUNTY OF HUMBOLDT
Upon motion of Supervisor Lovelace Seconded by Supervisor Bass
Ayes Sundberg, Lovelace, Fennell, Bohn, Bass
Nays
Abstain
Absent

and carried by those members present, the Board hereby approves the recommended action contained in this Board report.

Dated: Dec. 8, 2015
By:
Kathy Hayes, Clerk of the Board

financially eligible children under age 21 with certain physical limitations and chronic health conditions or diseases.

For CCS to make eligibility decisions for their clients, it is necessary to access medical records from a variety of medical treatment centers. UCSF Benioff Children's Hospital Oakland (CHO) is one of the primary medical centers treating children from Humboldt County. CHO has implemented an online medical records portal and has requested all providers to access records electronically. They are no longer responsive to faxed records requests or phone calls, as they are phasing out non-electronic access methods. This is causing delays in the ability of the CCS program to make eligibility decisions for clients, which is a barrier to accessing medically necessary services for very sick children.

The agreement spells out the confidentiality and other requirements users of the CHO remote access link must adhere to, as we will be accessing protected health information (PHI) held by CHO, and it obligates the County to comply with certain terms and conditions pertaining to accessing PHI. This is a one way exchange of information – CHO will not have access under this agreement to protected health information held by Public Health.

CHO requested that the County of Humboldt sign the agreement first. They will return two fully executed originals to Humboldt County DHHS, and Public Health will forward a complete copy of the contract to the Board.

FINANCIAL IMPACT:
The agreement with CHO does not have any associated costs. There is no impact to the General Fund.

This agreement supports the Board's Strategic Framework by protecting vulnerable populations and creating opportunities for improved safety and health.

OTHER AGENCY INVOLVEMENT:
There are no other agencies involved in this agreement.

ALTERNATIVES TO STAFF RECOMMENDATIONS:
The Board could choose not to approve this Agreement. However, this is not recommended as CCS is a mandated State program and it would greatly restrict our ability to make eligibility decisions for clients and to provide medically necessary services for very sick children.

ATTACHMENTS:
Three (3) original agreements with UCSF Benioff Children's Hospital Oakland

Remote Access Service Agreement for EpicCare Link

This Remote Access Service Agreement ("Agreement") is made as of this _____ date of 2015 (the "Agreement Effective Date") by and between County of Humboldt, a political subdivision of California ("REQUESTOR"), and UCSF Benioff Children's Hospital Oakland ("CHILDREN'S") for the purpose of granting REQUESTOR secure access to CHILDREN'S electronic medical record through EpicCare Link as described herein and incorporated into this Agreement.

RECITALS

1. CHILDREN'S has an interest in improving the delivery and coordination of care to its patients by providing secure electronic access to select portions of its patients' medical records as contained in the CHILDREN'S electronic medical record ("EMR") to authorized providers and external entities using EpicCare Link software.

2. REQUESTOR desires to obtain access to the CHILDREN'S EMR to provide care/service to its patients/clients through the use of EpicCare Link software.

3. CHILDREN'S and the REQUESTOR desire to protect the privacy and provide for the security of PHI accessed via EpicCare Link in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act");and regulations promulgated thereunder by the U.S. Department of Health and Human Services ("HIPAA Regulations"), the California Confidentiality of Medical Information Act ("COMIA"), California Civil Code Section 56 *et seq.*, and other applicable state and federal laws. (The laws will sometimes be collectively referred to herein as Confidentiality Laws.)

The parties therefore agree as follows:

AGREEMENT

1. **Access to CHILDREN'S EMR via EpicCare Link.** Upon execution of this Agreement and any other required documents, and approval of all access sites and Users as required herein, CHILDREN'S will provide the REQUESTOR with passwords and information to allow it to access CHILDREN'S EpicCare Link solely for the REQUESTOR's patients/clients. CHILDREN'S will also provide limited training on the EpicCare Link system.

2. **Definitions**

   A. **Breach** shall mean the inappropriate access, review, or viewing of PHI without a direct need for medical diagnosis, treatment, or other lawful use as permitted by California Civil Code Section 56.10. Breach shall also have the meaning given to the term by 42 U.S.C. Section 17921 and 45 C.F.R. Section 164.402.

   B. **Individual** has the same meaning as the term in 45 C.F.R. Section 160.103 and refers to the person who is the subject of PHI.

   C. **Privacy Rule** shall mean the standards and implementation specifications for protecting the privacy of individually identifiable health information at 45 C.F.R. Parts 160 and 164, Subparts A and E, which implement certain provisions of HIPAA, the privacy provisions of the HITECH Act, and the regulations and guidance promulgated thereunder.

D. **Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an Individual or the provision of health care to an Individual; and (ii) that either actually identifies the Individual or with respect to which there is a reasonable basis (as determined by RAM) to believe the information can be used to identify the Individual; and (iii) shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501. PHI shall also include Patient Medical Information as defined by California Civil Code Section 56.05 and applied in California Health and Safety Code Section 130203.

E. **Protected Information** shall mean PHI provided by CHILDREN'S to REQUESTOR or created or received by REQUESTOR on CHILDREN'S behalf.

F. **Required by Law** has the same meaning as the term in 45 C.F.R. Section 164.103.

G. **Remote Access Management (RAM)** means the unit within the Hospital Information Systems (HIS) department that manages remote access.

H. **Security Incident** has the same meaning as the term in 45 C.F.R. Section 164.304, and refers to a breach of security.

I. **Security Rule** shall mean the HIPAA Regulations that are codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

J. **User** shall mean a user connecting to CHILDREN'S EpicCare Link software from the internet.

3. **Children's Propriety Information.** CHILDREN'S EpicCare Link contains PHI which is the sole property of CHILDREN'S. The parties agree and understand that this PHI of CHILDREN'S patients ("CHILDREN'S PHI") will remain the property of CHILDREN'S, and that there is no intent to transfer any rights or legal interest in CHILDREN'S PHI to the REQUESTOR by virtue of this agreement. REQUESTOR agrees that it will not copy or utilize CHILDREN'S PHI for any purpose except to coordinate the patient/client's treatment and/or payment for services, unless CHILDREN'S consents in writing or such use or disclosure is required by law. ***If the REQUESTOR receives a request or demand for disclosure of CHILDREN'S PHI, it will immediately provide written notice and a copy of such request or demand to CHILDREN'S as set forth in paragraphs 6(E) and 12(E).***

4. **Permitted Use of CHILDREN'S PHI.** REQUESTOR understands that CHILDREN'S PHI contains confidential patient information, and its disclosure is governed by the Confidentiality Laws. REQUESTOR is permitted to use CHILDREN'S PHI only for purposes related to coordination of REQUESTOR'S patient/client's treatment and/or payment for services.

5. **Prohibited Uses of CHILDREN'S PHI.** REQUESTOR agrees it will not access or use CHILDREN'S PHI for any purpose other than those set forth in paragraph 4 above Specifically, REQUESTOR may not:

   A. Sell, disclose to any third party, transfer to any third party or otherwise permit or facilitate third-party access to CHILDREN'S PHI.

   B. Transmit in any way CHILDREN'S PHI through the CHILDREN'S EpicCare Link for any purpose other than those listed in paragraph 4.

C. Use any CHILDREN'S PHI with the intent to negatively impact the competitive advantage of CHILDREN'S in the marketplace;

D. Use or disclose CHILDREN'S PHI other than as permitted by this Agreement.

If CHILDREN'S determines that REQUESTOR has accessed or used CHILDREN'S PHI in a prohibited or unlawful manner, CHILDREN'S may unilaterally terminate all access to EpicCare Link, and seek any such other relief as appropriate.

6. **Confidentiality of CHILDREN'S PHI:** REQUESTOR agrees to comply with the Confidentiality Laws in its use of CHILDREN'S PHI and to take all reasonable and necessary measures and precautions as required by those laws to ensure the security and privacy of CHILDREN'S PHI it accesses. Specifically, REQUESTOR agrees to:

   A. Immediately report to RAM any unauthorized use of disclosure of any portion of CHILDREN'S PHI of which REQUESTOR becomes aware;

   B. Advise patients requesting amendments to their medical records that REQUESTOR does not have the authority or the ability to alter their CHILDREN'S PHI, and that any such requests must be directed to CHILDREN'S;

   C. Take appropriate precautions to ensure that patients, clients, visitors or unauthorized personnel will not be able to see the computer screens during access to CHILDREN'S PHI.

   D. Make its internal practices, books and records relating to the use and disclosure of PHI or CHILDREN'S PHI available to CHILDREN'S, and after notice, to the Secretary of Health and Human services for the purposes of determining CHILDREN'S compliance with privacy regulations;

   E. If it receives a request for disclosure of CHILDREN'S PHI from a court or governmental agency, REQUESTOR will immediately notify the RAM prior to making any disclosure, in order to allow CHILDREN'S the opportunity to seek an appropriate protective order to protect CHILDREN'S PHI.

7. Obligations of REQUESTOR

   A. REQUESTOR is solely responsible for the cost of the equipment, maintenance, and supplies required for access to and use of CHILDREN'S PHI through CHILDREN'S EpicCare Link.

   B. REQUESTOR agrees it will not change or alter the Service software in any way. In the event REQUESTOR suspects any problems related to unauthorized data alterations or destruction, REQUESTOR will instruct its Users to immediately discontinue using the Service and report the problem to RAM.

   C. Prior to obtaining access, REQUESTOR will provide a written list to RAM identifying the Users who will be authorized by REQUESTOR to access CHILDREN'S PHI. The RAM will advise the REQUESTOR of the specific information needed to set up User access. REQUESTOR agrees that it will ensure that Users only access CHILDREN'S PHI pursuant to this Agreement. If additional Users are desired, or if a User needs to be removed for any reason, REQUESTOR contact RAM to effect these changes.

   D. REQUESTOR agrees to ensure that its Users read the Privacy, Confidentiality, and Security Handbook, which is attached hereto as Exhibit A and incorporated herein by

reference, print and sign the acknowledgment page, and return the acknowledgment page to HIS prior to the User being provided remote access. REQUESTOR further agrees to ensure that its Users sign the EpicCare Link Terms and Conditions document[1] and access CHILDREN'S PHI in accordance with the terms of this Agreement and CHILDREN'S policies as outlined in the Privacy, Confidentiality and Security Handbook and the EpicCare Link Terms and Conditions.

E. REQUESTOR will take steps to discontinue a User's access in the event it determines that the User improperly accessed or used CHILDREN'S PHI or shared passwords with an individual not identified as a User in violation of law or this Agreement.

F. REQUESTOR is required to ensure that its Users are educated and trained about the limitations on the access to and use of Children's PHI required by the Confidentiality Laws.

G. REQUESTOR represents that it is in compliance with all applicable state and federal laws and regulations governing providers of healthcare to patients, and neither it nor any of its Users, employees, agents or business entities has been debarred, penalized, convicted, sanctioned, suspended, excluded or otherwise deemed ineligible to participate in any state or federal reimbursement program, including Medicaid (MediCal) or Medicare. In the event that REQUESTOR or any of its Users, employees, agents or officers are sanctioned or excluded from participation in any state or federal reimbursement program as described above, REQUESTOR will immediately notify RAM.

8. **Assignment.** Neither this Agreement nor any of the rights herein may be assigned by REQUESTOR without the express, prior written approval of CHILDREN'S. CHILDREN'S may, without the consent of REQUESTOR, assign the rights and obligations herein to any entity affiliated with CHILDREN'S.

9. **Relationship of the Parties.** It is expressly understood and agreed that this Agreement is not intended to, and does not, create a joint venture, partnership, association or other affiliation or business relationship between the parties. CHILDREN'S and REQUESTOR shall at all times be separate legal entities and are not liable for the debts or obligations of the other party.

10. INSURANCE AND LIABILITY

A. **Insurance.** Each party, at its sole cost and expense, shall insure its activities in connection with this Agreement. Specifically, REQUESTOR and CHILDREN'S shall each obtain, keep in force and maintain insurance or equivalent programs of self-insurance with appropriate limits that shall cover losses that may arise from breach of this Agreement, breach of security, or any unauthorized use or disclosure of PHI. It should be expressly understood, however, that the insurance required herein shall in no way limit the liability of REQUESTOR or CHILDREN'S with respect to its activities in connection with this Agreement.

B. **Indemnification by REQUESTOR.** REQUESTOR agrees to defend at CHILDREN'S election, indemnify, and hold harmless CHILDREN'S, its officers, agents and employees from and against any and all claims, liabilities, demands, damages, losses, costs and expenses, (including costs and reasonable attorneys' fees) or claims for injury or damages that are caused by or result from the acts or omissions of REQUESTOR, its

[1] The EpicCare Link Terms and Conditions document is acknowledged at the time the User signs on to EpicCare Link for the first time.

officers, agents or employees with respect to the use and disclosure of CHILDREN'S PHI.

C. **Indemnification by CHILDREN'S.** CHILDREN'S agrees to defend at REQUESTOR'S election, indemnify, and hold harmless REQUESTOR, its officers, agents and employees from and against any and all claims, liabilities, demands, damages, losses, costs and expenses, (including costs and reasonable attorneys' fees) or claims for injury or damages that are caused by or result from the acts or omissions of CHILDREN'S, its officers, agents or employees with respect to the use and disclosure of CHILDREN'S PHI.

D. **Comparative Liability.** In the event that both parties are held to be negligently or willfully responsible, each party will bear its proportionate share of liability as determined in any such proceeding. In such cases, each party will bear its own costs and attorneys' fees.

E. **Violations.** REQUESTOR acknowledges that if it violates any of the requirements of this Agreement, REQUESTOR will be subject to the same civil and criminal penalties that CHILDREN'S, as a Covered Entity, would be subject to if CHILDREN'S violated the same requirements.

11. TERM AND TERMINATION

The term of this Agreement shall begin on the Agreement Effective Date and will continue in full force and effect for three (3) years, unless sooner terminated as provided herein.

A. This Agreement may be terminated:

i) at any time by REQUESTOR by giving 15 days' written notice to CHILDREN'S;

ii) by CHILDREN'S if REQUESTOR materially breaches any obligation in the Agreement, and the breach either cannot be cured or, in the case of a breach that is curable, is not cured within 15 days of receiving written notice from CHILDREN'S;

iii) by CHILDREN'S, at its option and without cause, upon delivery by CHILDREN'S of 60 days' written notice to REQUESTOR;

iv) at any time by mutual consent in writing.

Termination of this Agreement with respect to REQUESTOR shall apply to any and all agreements permitting REQUESTOR's Users to have access to CHILDREN'S EpicCare Link.

B. **Effect of Termination.** Upon termination of this Agreement for any reason, REQUESTOR, with respect to PHI received from CHILDREN'S, or created, maintained, or received by REQUESTOR on behalf of CHILDREN'S, shall:

i) Retain only that CHILDREN'S PHI which is necessary for REQUESTOR to continue its proper management and administration or to carry out its legal responsibilities;

ii) Return to CHILDREN'S or destroy the remaining CHILDREN'S PHI that REQUESTOR still maintains in any form;

iii) Continue to use appropriate safeguards and comply with the Confidentiality Laws to prevent use or disclosure of CHILDREN'S PHI, other than as provided for in this Section, for as long as REQUESTOR retains CHILDREN'S PHI;

iv) Not use or disclose CHILDREN'S PHI retained by REQUESTOR other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section 4 above, which applied prior to termination; and

v) Return to CHILDREN'S or destroy CHILDREN'S PHI retained by REQUESTOR when it is no longer needed by REQUESTOR for its proper management and administration or to carry out its legal responsibilities.

C. **Injunctive Relief.** The parties hereto understand and agree that the terms of this Agreement are reasonable and necessary to protect the interests of CHILDREN'S and REQUESTOR. The parties further agree that CHILDREN'S would suffer irreparable harm if REQUESTOR breached this Agreement. Thus, in addition to any other rights or remedies, all of which shall be deemed cumulative, CHILDREN'S shall be entitled to obtain injunctive relief to enforce the terms of this Agreement.

12. MISCELLANEOUS PROVISIONS

A. **Disclaimer.** CHILDREN'S makes no warranty or representation that compliance by REQUESTOR with this Agreement, or the Confidentiality Laws will be adequate or satisfactory for REQUESTOR'S own purposes. REQUESTOR is solely responsible for all decisions made by REQUESTOR regarding the safeguarding of PHI.

B. **No Third Party Beneficiaries.** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CHILDREN'S, REQUESTOR, and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

C. **Notice to Secretary.** If CHILDREN'S knows of a pattern of activity or practice of REQUESTOR that constitutes a material breach or violation of REQUESTOR'S obligations under this Agreement, if the material breach or violation continues, and if termination of this Agreement is not feasible, CHILDREN'S is required by the HIPAA Regulations to report the breach or violation to the Secretary of Health and Human Services.

D. **Survival.** To the extent required by law, the obligations of REQUESTOR shall survive the termination of this Agreement.

E. **Notices.** Any notices to be given to either party shall be made in writing and sent via certified U.S. Mail, return receipt requested, or by express courier to the address given below. Notice shall be effective upon actual receipt or refusal as shown on the receipt obtained pursuant to the foregoing.

UCSF Benioff Children's Hospital Oakland
747 Fifty Second Street
Oakland, CA 94609

Attention: _____
Remote Access Management
cc: General Counsel

County of Humboldt
DHHS – Public Health
529 I Street
Eureka, CA 95501

Attention: Susan Buckley
Public Health Director

Each party may change its address and its representative for notice by giving notice in the manner provided above.

F. **Conflicting Terms.** To the extent that there is any conflict between the terms of this Agreement and the terms of other agreements in place between REQUESTOR and CHILDREN'S, the terms of this Agreement shall prevail. All non-conflicting terms and conditions of any other Agreement remain in full force and effect.

G. **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with applicable state and federal laws, regulations, and rules (including, without limitation, the Confidentiality Laws).

H. **Severability.** If any provision of this Agreement shall be declared invalid or illegal for any reason whatsoever, the remaining terms and provisions of this Agreement shall remain in full force and effect in the same manner as if the invalid or illegal provision had not been contained herein, and such invalid, unenforceable, or illegal provision shall be valid, enforceable, and legal to the maximum extent permitted by law.

I. **Application of State Law.** Where any applicable provision of California law relates to the privacy of health information and is not preempted by HIPAA, as determined by application of the HIPAA Regulations, the parties shall comply with the applicable provisions of California law.

J. **No Private Cause of Action.** This Agreement is not intended to and does not create a private cause of action by any Individual, other than the parties to this Agreement, as a result of any claim arising out of a breach of this Agreement, the HIPAA Regulations, or other state or federal law or regulation relating to privacy or confidentiality.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Agreement Effective Date

UCSF Benioff Children's Hospital Oakland	**County of Humboldt**
_____	Estelle Fennell
Signature	Signature
_____	Estelle Fennell
Printed Name	Printed Name
_____	Chair,
Title	Humboldt County Board of Supervisors
	Title
_____	12/8/2015
Date	Date
_____	K Vizgaudis
Signature	Signature
_____	Kelly Vizgaudis
Printed Name	Printed Name
_____	Risk Manager
Title	Title
_____	11/19/15
Date	Date

EXHIBIT A

CHILDREN'S HOSPITAL
& RESEARCH CENTER OAKLAND

Privacy, Confidentiality, and Security Handbook

A GUIDE FOR EMPLOYEES, MEDICAL STAFF,
STUDENTS, TRAINEES, AND VOLUNTEERS

PRIVACY, CONFIDENTIALITY & SECURITY OF INFORMATION POLICY

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's, its patients, activities and affiliates, in accordance with the law and Children's policy.

I agree to access, use, or disclose confidential information only in the performance of my Children's duties, where required – 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 Children's-related purposes. I will not knowingly discuss any confidential information within the hearing of 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 which is incidentally disclosed to me in the course of my relationship with Children's.

I understand that psychiatric records, drug abuse records, 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 Children's 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 this to Hospital Information Systems and request a new password.

I understand that violation of any of the 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 of 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**
Print Name	**Department**

Resources are available throughout Children's Hospital to answer questions and guide you on various matters.
When you have questions pertaining to any topic described within this booklet, the following contact is available:

COMPLIANCE & PRIVACY OFFICER
DIRECTOR, MEDICAL RECORD DEPARTMENT
COMPLIANCE HOTLINE
LEGAL AFFAIRS

LETTER FROM THE PRESIDENT

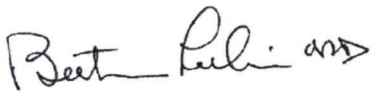
Dear Fellow Employees,

At Children's Hospital & Research Center Oakland it is our privilege to care for children and their families, often during trying times. The quality of the care we provide depends on our ability to access, document, and communicate accurate medical information about our patients. It also depends on our sensitivity and respect for the privacy and confidentiality of the kids and families we serve.

Privacy can be difficult to define and expectations vary among individuals and cultures. Federal and state laws offer some universal guidance to protecting patient information, privacy, and confidentiality. This handbook will introduce you to the privacy and security regulations established by the federal Health Insurance Portability and Accountability Act (HIPAA) and by the California Confidentiality of Medical Information Act (CMIA). These regulations apply to all hospital faculty, staff, students, and volunteers.

We are giving this book to every employee and affiliate of Children's Hospital because it is essential that each of us demonstrate sensitivity to the privacy of others in all we do. Please read this handbook to gain a basic understanding of the federal and state laws and how they affect what we do at Children's. Training designed to address specific jobs will be available to supplement this handbook and help orient all new and existing faculty, staff, students, and volunteers.

We have a legal duty to comply with these regulations. More importantly, we have an ethical duty to respect the privacy and confidentiality of the people we serve. Thank you for doing your part to make Children's an organization of which we can all be proud.



Bertram H. Lubin, MD
President and Chief Executive Officer

OVERVIEW: PRIVACY AND CONFIDENTIALITY

What is HIPAA?

The acronym "HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996. HIPAA is a federal law designed to **protect the privacy** of patient information, to **provide for the electronic and physical security** of health and patient medical information, and to **simplify billing and other electronic transactions** through the use of standard transactions and code sets (billing codes).

What do HIPAA administrative simplification rules cover?

The HIPAA administrative simplification rules include:

- uniform electronic transaction standards for healthcare data;
- privacy and confidentiality provisions for individually-identifiable healthcare data;
- security procedures to protect electronically maintained health information;
- National Provider Identifier (NPI) unique health identifiers for providers, employers, plans, and individuals to be used when complying with the electronic transaction standards.

When did the HIPAA rules take effect?

Patient privacy rules: April 14, 2003
Electronic transaction standards: Oct. 16, 2003
Security rules: April 21, 2005
National Provider Identifier use: May 23, 2007

Do HIPAA rules apply to me?

The law applies to hospitals, other healthcare delivery organizations, and health plans, as well as to physicians, other care providers, employees, and other members of the workforce of these institutions.

What do HIPAA privacy rules cover?

Many of the rights granted to patients and their parents/guardians by the HIPAA privacy rules have existed for years under California law.

New provisions guarantee the rights of parents/guardians to:

- request access to their child's medical information;
- ask to amend the information in their child's medical record;
- receive an accounting of disclosures of their child's health information

Privacy rules also require healthcare organizations to:

- appoint a privacy officer/committee;
- establish administrative, technical, and physical safeguards for protected information;
- provide parents/guardians with a *Notice of Privacy Practices* explaining how the organization will handle medical information;
- make a "good-faith" effort to obtain a written acknowledgement of the parent's/guardian's receipt of the *Notice of Privacy Practices;*
- use "need to know" and "minimum necessary" standards in determining whether hospital faculty, staff, students, trainees, and volunteers may access protected health information.

What are the potential consequences of not complying with the law?

Showing disrespect for patient privacy and confidentiality damages Children's Hospital & Research Center Oakland's (Children's) excellent reputation and runs contrary to the values held by the hospital and its community.

HIPAA also imposes penalties and fines for breaches of privacy. Breach of Children's policies can result in disciplinary actions, including termination of employment or professional relationship with Children's.

External investigations of violations can result in serious penalties. For example, an individual found guilty of releasing confidential information for personal gain (such as selling information about a celebrity to a newspaper) could be fined $250,000 and be imprisoned for 10 years. A privacy violation may lead to costly lawsuits.

CONFIDENTIAL INFORMATION

What is confidential protected health information (PHI)?

Information that can be matched with a patient; is created in the process of caring for the patient; and is kept, filed, used, or shared in an electronic (ePHI), written or oral manner is information that we must protect.

Examples of PHI include a patient's:

- name
- address
- birth date
- age
- medical record number
- phone and fax numbers
- e-mail addresses
- medical records
- diagnoses
- x-rays, photos, and other images
- prescriptions
- lab work and test results
- billing records, claim data, referral authorizations, and explanation of benefits
- research records of patient care

Who may access confidential PHI?

Doctors, nurses, and other licensed providers in a patient's healthcare team may access that patient's entire medical record, based on their "need to know." All other members of our workforce have access only to the information they need to perform their job duties.

I'd like to remind a patient of her appointment. Can I use confidential PHI?

Yes. Issuing an appointment reminder ensures our ability to provide quality treatment and services to our patients. It is a valid reason to use PHI without specific authorization.

What is the "minimum necessary" standard?

You must use the "minimum necessary" standard when accessing PHI. For example, while physicians, nurses, and other providers may need to view the entire record to provide adequate care, 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. Please access and use only the patient information that you need to perform your job well.

When may I use PHI without authorization?

We must remain mindful of patient privacy at all times. We may use PHI, without seeking the parent's/guardian's authorization, only for specific reasons, including:

- to provide medical **treatment** or services;
- to obtain **payment for** these services;
- to help us with healthcare and business **operations** and to ensure the quality of care we provide;
- to meet a legal requirement to disclose information.

We often refer to these reasons by the acronym TPO, which stands for treatment, payment, and (healthcare) operations.

Healthcare and business operations are broad terms. What do they include?

Such operations include a wide array of activities from teaching and healthcare communications between a family and the patient's physician to fundraising efforts on behalf of Children's, planning and development, and creating a hospital directory.

Someone else broke the rules and I learned about it. What should I do?

We have an ethical responsibility to respect the privacy and confidentiality of our patients. Children's Code of Conduct states that each of us must prevent unauthorized or unapproved access to—or disclosure of—patient information. Report concerns to your supervisor, the Children's Compliance Hotline at 510-428-3234, or the Children's Privacy Officer at 510-428-3574.

If health-related information is de-identified (*i.e.* if all personal identifiers are removed), it is not PHI and may be shared without restriction.

When do I need to obtain written authorization?

To use or disclose PHI for almost any reason other than treatment, obtaining payment, or hospital operations, you must obtain a written authorization from the patient prior to access or disclosure. Please refer to the *Notice of Privacy Practices* for a list of covered exceptions to the authorization requirement related to public policy, certain health disease reporting requirements, and law enforcement activities.

Residents, students, and trainees: access to PHI

Residents, students, and trainees are required to complete a privacy orientation and to sign a confidentiality agreement. If you are a resident, student, or a trainee, you may *never* remove any PHI from Children's premises. You may request copies of de-identified data for use in case presentations; however, the request for use/disclosure must be coordinated with the Medical Record Department.

MEDICAL RECORD ACCESS AND CONTROL

We maintain medical records for the benefit of the patient, medical staff, and the hospital. Medical records are made available when requested by:

- the admitting, attending, and other physicians (including residents) who are involved in the patient's direct care;
- non-physicians involved in the patient's direct care, such as nurses or pharmacists;
- any authorized officer, agent, or employee of Children's or its medical staff, such as members of the Risk Management and Legal Affairs department;
- Children's researchers, when the request is part of an approved Internal Review Board (IRB) protocol that involves medical record review;
- any other person authorized by law to make such a request (medical examiners, law enforcement officers, regulatory agencies);
- the patient's parent/guardian or other authorized representative.

A child's medical information belongs to that child and her parent or guardian. However, the child's health record is the physical property of Children's. A medical record may be removed from Children's jurisdiction only by a subpoena, a court order, or a statute.

Only authorized Medical Record Department staff may remove medical records from patient care areas. In some cases an established administrative or Medical Record Department policy may authorize the removal of records from patient care areas. Medical information held in paper form must be stored in secure areas. Please make sure that you never leave medical information in locations where unauthorized users can access it.

You must use the bin specially designated for confidential materials when discarding medical information that is no longer needed. You may also shred it, ensuring that the information on the shredded paper is no longer identifiable.

How can I protect the confidentiality and security of health information?

- Destroy all paper that contain PHI. Always follow the proper paper disposal procedure. Locked confidential disposal bins are located throughout Children's.
- Review and abide by the Children's Confidentiality Statement (Appendix II).
- File documents away when you have finished using them:
  - Keep confidential or sensitive information locked away when not in use
  - Clear a workstation before leaving it
  - Always follow the visitor security procedure
  - Always wear a security/identity badge at work
  - Never leave sensitive or confidential information in a trash bin
  - Be alert to recognize and correct privacy breaches.

COMPUTER SYSTEMS & ELECTRONIC TRANSMISSIONS OF INFORMATION

We must secure the information we possess in order to protect its confidentiality, integrity, and availability. We must ensure that information:

- doesn't fall into the wrong hands;
- is not damaged, corrupted, or destroyed;
- can be made available to the right people at the right time.

The Children's Hospital Information Systems (HIS) department helps secure the electronic and physical access to ePHI by establishing security policies and systems to protect our computers from hackers. These systems safeguard against malice, but not against carelessness. Sharing or posting passwords or violating hospital technology security policies endangers the confidentiality of ePHI.

How can I protect the confidentiality and electronic security of health information?

There are steps that you must take to help protect patient information:

- Never share or post passwords.
- Remember your password; do not write it down.
- Log off of computer stations when finished.
- Review and abide by the Children's Confidentiality Statement (Appendix II).
- Clear a workstation before leaving it;
- Always follow the visitor security procedure;
- Always wear a security/identity badge when at work;

- Never leave sensitive or confidential information in a trash bin;
- Be alert to recognize and correct privacy breaches.

Electronic Communication

When using e-mail, voice mail, answering machines, telephones, faxes, and mobile computing devices to store or communicate patient information you must be cautious. Below are rules you must follow to ensure the security of patient information.

E-Mail

- Assume normal e-mail systems are not secure, unless you have specific and clear information that the system is encrypted or in other ways secured.
- Consider carefully what you send via e-mail.
- Do not send confidential information unless you can de-identify it.
- Warn patients who communicate with you via e-mail that their confidentiality cannot be ensured.
- 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.
- Do not send attachments containing protected health information without encryption.
- Add a confidential message footer to your messages.

COMPUTER SYSTEMS & ELECTRONIC TRANSMISSIONS OF INFORMATION

Voice Mail, Answering Machines, and Telephone Communication

- Consider who has access to your voice mail or answering machine to ensure others do not access PHI.
- Do not leave PHI on answering machines and voice mail, unless the patient has authorized you to do so.
- If you use the speakerphone, be aware of you surroundings and sensitive to the messages being replayed.

FAX

- Never fax information to an unsecured fax machine. Only fax machines located in a restricted environment are secure. Call ahead to ensure that the intended recipient will pick up the fax.
- Always check the destination fax number before faxing.
- Use Children's's standard fax cover sheet containing a confidentiality statement. This is automatically included with reports faxed from Meditech. For other faxed reports use the statement in the sidebar (right).
- Return items you received by mistake and advise sender of the error.

Sample Confidential E-mail Message Footer

***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.*

Sample Confidential fax Message

***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.*

Mobile Computing Devices Containing PHI

- Never leave equipment in an exposed or unsecured area.
- Always password-protect portable equipment such as laptops and personal data assistants (PDAs).
- Frequently make protected backups of data stored on remote systems.
- Never leave information or information systems containing PHI open to access while unattended.
- When accessing PHI at off-site and/or home offices, follow security and privacy practices similar to those in effect at Children's.
- Use caution when uploading or downloading files to/from PDAs. Adhere to the "minimum necessary" standard.

Password Security

- Keep your password secret.
- Never lend your system password to another person.
- Commit your password to memory.
- If the system you are using does not periodically change your password, do so yourself.

CONFIDENTIALLY SPEAKING

Respecting patient privacy and confidentiality is an important aspect of providing good service and quality care. Sharing patient information with each other in hallways, elevators, on the streets, in restaurants and other public areas compromises the privacy of our patients. Even when you think you are discussing a patient without clear-cut identifiers, you may be breaching the patient's privacy.

Our patients have told us their privacy is important to them. Let them know we respect their privacy, too. Please be mindful of patient confidentiality.

- *Knock and wait to be acknowledged before entering patient and treatment rooms; introduce yourself.*
- *Hold all patient information discussions in a private location. Do not discuss patients in public areas such as elevators, the cafeteria, or in the hallways.*
- *Share information about patients only with those who have a valid reason to know. Never publicly disclose private facts about a patient or a family.*
- *Let patients know when you do something to enhance their privacy, such as pulling a curtain, closing doors, and speaking softly.*

THE RIGHTS OF OUR PATIENTS

The *Notice of Privacy Practices* describes in detail the patient's rights under HIPAA. All patients will receive a copy of this notice when they come to the hospital for service. The notice is also available on Children's's website, www.childrenshospitaloakland.org. We are required to make a good faith effort to obtain the patient's acknowledgement of receipt. Remember, in a pediatric setting, the patient's rights are often exercised by the patient's parent or guardian.

Here are brief descriptions of the rights of our patients. The *Notice of Privacy Practices* and the brochure *Your Child's Medical Information* explain in detail how patients can exercise their rights.

Right to Inspect and Copy: Patients may inspect and for a fee, may request copies of their medical record.

Right to Request an Amendment: Patients who feel that information we have about their children is incorrect or incomplete may ask us to amend the information.

Right to an Accounting of Disclosures: Patients may request a list of certain types of disclosures of medical information about them.

THE RIGHTS OF OUR PATIENTS

Right to Request Restrictions: Patients may request a restriction or limitation on the medical information we use or disclose about their children for treatment, payment, or healthcare operations. They may also request limits on the medical information we disclose to people involved in their children's care or the payment for the care, such as family members or friends.

Right to Request Confidential Communication: Parents/guardians may request that we communicate with them about medical matters in a certain way or at a certain location. For example, they may ask that we only contact them at work or by mail.

Right to File a Complaint: Patients may file a complaint if they think that their privacy rights have been violated.

Right to a Paper Copy of Privacy Notice: Patients may ask for a paper copy of the *Notice of Privacy Practices* at any time.

PATIENT DIRECTORIES

Upon admission to Children's, we list a child's name, time of admission, location in the hospital, general condition (good, fair, serious, or critical), and religion in our hospital directory. Only individuals who ask about a child by name have access to this information. We disclose a child's religion only to members of the clergy.

We use the information in the directory to assist visitors and delivery staff, such as florists, find a child's room. We also refer to the directory to respond to general questions about a child's condition.

Someone called to ask about the condition of a child by name. The child is listed as a "confidential patient." How should I respond?

Respond to inquiries (in person, writing, or by phone) about "confidential patients," by saying "We have no information concerning this patient." If the caller or visitor persists, refer him to your supervisor or house supervisor after hours. Social Services can also be of assistance in working through particularly sensitive issues. The caller or visitor may also be referred to Risk Management.

Confidential Patients

When a child is designated as a "confidential patient" no information may be released or divulged concerning the child's diagnosis, condition, or presence in the hospital. HIPAA grants parents/guardians the right to request a "confidential patient" designation. No directory information may be given out in response to inquiries about "confidential patients."

AUTHORIZATIONS

HIPAA specifies the content of an authorization to disclose PHI. Children's must have a valid written authorization for the disclosure or access of PHI for uses other than treatment, payment, and healthcare operations.

Who can authorize the use or disclosure of PHI?

In most situations, parents, guardians and/or others with legal responsibilities for minors (children under 18 years of age) may authorize the use or disclosure of medical information on behalf of the minor. There are situations in which minors independently may exercise their rights as described in the *Notice of Privacy Practices.*

Certain types of PHI, such as HIV information and psychotherapy records, require specific authorization. Special rules also apply for research.

If you are unsure about whether a request of information is authorized, always check with your manager or the Release of Information section in the Medical Record Department. These disclosures may be subject to a request for an accounting of disclosures, so the requests need to be coordinated, tracked, and clearly documented.

DE-IDENTIFICATION OF PHI

Children's employees must make all reasonable efforts to limit the use or disclosure of PHI. PHI that has been de-identified may be used without restrictions and without an authorization.

The de-identification rule states that you can disclose health information after it is no longer PHI because the 19 identifying data elements listed in the regulations have been removed. (See Appendix 1 for a list of the 19 data elements).

Another class of information referred to as a "limited data set" is PHI that excludes 16 of the 19 identifiers. (See Appendix I for data elements allowed for use.) The limited data set can be used for research and public health or healthcare operations, as long as the recipient of the data signs a data use agreement with Children's.

BUSINESS ASSOCIATES

Some of the services or activities in our organization are provided through contracts with business associates. For example, we may contract with accreditation agencies, management consultants, quality assurance reviewers, billing and collection services, and accountants to provide services on our behalf. We may disclose medical information to our business associates so that they can perform the service on our behalf.

We require our business associates to sign a written privacy agreement. Refer all purchase orders or agreements involving protected health information to either Material Management or the Risk Management and Legal Affairs departments for review. Do not agree to sign or authorize another vendor's business associate agreement or "trading partner agreement." Instead, refer the business associate to Risk Management and Legal Affairs. Risk Management and Legal Affairs department staff must review all contracts. At that time, a Business Associate Agreement will also be generated.

CLINICAL RESEARCH AND OTHER RESEARCH INVOLVING HUMAN SUBJECTS

Children's is a research institution. All research projects conducted by the hospital must be approved through a special review process to protect patient safety, welfare, and confidentiality. A child's medical information may be important to further research efforts and the development of new knowledge. We may use and disclose medical information about our patients for research purposes, subject to the confidentiality provisions of state and federal law. Occasionally, researchers contact patients regarding their interest in participating in certain research studies. Enrollment in those studies can only occur after the parent/guardian has been informed about the study, had an opportunity to ask questions, and has signed a consent form for the child's participation in the study. When approved through a special review process, other studies may be performed using the child's medical information without requiring consent.

How will HIPAA affect research at Children's?

At Children's, the Institutional Review Board (IRB) also serves as the Privacy Board that reviews all uses and disclosures of PHI for research purposes. For many research projects, the transition to HIPAA will be relatively simple, as the IRB already has policies that are HIPAA-compliant. Guidance for

The research protocol of my study was approved prior to April 14, 2003 when HIPAA took effect. How does this affect my use of PHI?

Although HIPAA privacy issues will have an impact on research, Children's will allow, in most cases, research protocols approved by the IRB prior to April 14, 2003, to use protocol PHI until the protocol's next annual renewal. However, any new subjects enrolled after April 14, 2003 will have to sign either an authorization for use and disclosure of PHI for research purposes or a modified informed consent document approved by the IRB.

research investigators will be added to the IRB Intranet site as the policies and procedures become available. The website will include templates for consent forms and protocols, authorization forms, detailed instructions, and a contact for investigators.

However, the expanded protection of health information will impose some changes on research studies, whether they are routine clinical studies or tissue/data repositories. The area most strongly affected by HIPAA is the identification and recruitment of potential research subjects through medical record searches or searches of other databases containing PHI. Other changes include HIPAA limitations on the sharing of PHI and on electronic transmission and physical security of the PHI, as well as specific privacy issues that must be addressed in the research protocol and in informed consent documents. With IRB approval, clinical databases, data repositories, and tissue and specimen banks can continue to be developed for research purposes and be maintained in perpetuity as long as they are HIPAA compliant. However, if IRB approval is not already in place, then IRB approval will need to be obtained prior to formation of these repositories and databases. The Medical Record Department will control the access to medical records for research protocols involving chart review or decedent research.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR MARKETING, FUNDRAISING, AND THE MEDIA

My department is offering lectures for parents on selected topics in autism? May we use PHI to publicize the class?

Because the information you will present relates to treatment options, you may use PHI, such as names, addresses, and diagnoses to send a calendar of upcoming classes.

Marketing

You may use PHI for communication relating to treatment options and health plan coverage. Use of PHI for other marketing purposes will require the patient's prior written authorization. If you are unsure about what PHI may be disclosed for marketing purposes, call the Communications department at 510-428-3367.

Fundraising

Both HIPAA and California law strictly limit the way hospitals can use PHI for fundraising purposes, including HIPAA-related training materials. The Children's Hospital Foundation oversees fundraising activities and events at Children's. Physicians, departments, divisions, and all other Children's entities should consult with foundation staff at 510-428-3814 before undertaking any fundraising activity.

Media

The Communications department is responsible for managing media relations and internal and external communications for Children's. If reporters, photographers or other media representatives call you with questions, please refer them to the main Communications number, 510-428-3367. Photographers, reporters, or camera crews cannot be in the hospital without supervision from the Communications department.

CASE SCENARIOS

Case 1: Breach of HIPAA Privacy
A nurse you are friendly with asks you what type of surgery is being performed on one of your patients. He is concerned about the patient because the child is his neighbor and the parent is a co-worker. What is the appropriate response to this situation?

Explanation: Since the nurse asked for the patient by name, you may refer the nurse to the hospital operator to obtain the hospital directory information available, which may include the patient's name and condition. Before disclosing any information, the operator will make sure the patient is not a "confidential patient."

Revealing the patient's diagnosis to this nurse without the prior oral and/or written consent from the child's parent/guardian is a breach of privacy. Disciplinary action may follow.

Ask yourself the following questions before giving out any patient information to friends, patient's family members, or co-workers:
1. Is the patient listed in the facility's records?
2. Has the parent/guardian consented to the release of directory information?
3. Does the requester have a "need to know"?
4. Do you have permission to disclose information to this person? If not, have you checked with the parent/guardian before giving out any information?
5. What is the minimum information necessary that you may provide?

6. Have you verified the person's identity before sending that person to the patient's room or disclosing information?

Case 2: Breach of HIPAA Privacy
You run into the parent of a former patient at the supermarket. She tells you that she had some cash flow problems and her bill was sent to collections. She mentions that her neighbor recently asked her if her child was fully recovered from surgery. The parent is upset because she never mentioned her child's surgery to anyone. It turns out that the parent's neighbor's son works for Children's's billing department.

Explanation: Report the incident to the Children's Privacy Officer. The Children's employee may have violated HIPAA, and the Privacy Officer must investigate the situation in coordination with the Human Resources department and compliance officer.

FREQUENTLY ASKED QUESTIONS

Q1. Other than the patient's medical record, are there types of PHI that we need to protect?

Examples of PHI that must be protected (in addition to the medical record) include:

- filled out prescription forms;
- faxed results from a reference laboratory and medical progress reports;
- copies of a consultant's report from another physician;
- face sheets with registration or other demographic information;
- medical billing records which identify the patient, e.g., HCFA-1500 claims, UB-92 claim;
- explanation of medical benefit statements (EOMBs) received from a payer;
- components of the medical chart, such as the initial intake form, progress notes, drug history or records kept in the outpatient/clinic chart;
- financial disclosures and waivers signed by the patient;
- eligibility lists received from an HMO;
- letters requesting progress notes from a medical director of a health plan;
- correspondence from a malpractice carrier regarding a patient;
- referral authorizations received from health plans;
- collection agency reports;
- e-mailed files from the transcriptionist;
- x-rays and other images.

FREQUENTLY ASKED QUESTIONS (FAQS)

Q2. Who is authorized to access PHI?

Physicians and other healthcare providers who are directly involved in the care of a patient may use PHI for the purposes of treatment, payment, and healthcare operations. These activities are described in the *Notice of Privacy Practices*. Physicians can disclose PHI to indirect care providers, such as consulting physicians, radiologists, and pathologists, but may not disclose PHI to clinicians who do not have direct or indirect treatment responsibilities. Providers and staff should exercise caution about disclosure of PHI to non-clinical staff members or providers who are not involved in the care of the patient. Access to PHI must be based on their job duties.

Q3. Why is an "incidental disclosure" of PHI not a violation of HIPAA?

Incidental uses or disclosures of PHI are not considered a violation of the HIPAA rules provided that Children's has met the reasonable safeguards and "minimum necessary" requirements. If these requirements are met, then hospitals may keep patient charts at bedside, doctors can talk to patients in semi-private rooms, and providers can confer at nurses' stations without fear of violating the rule if overheard by a passerby.

Who are considered business associates under HIPAA?

Examples of obvious business associates that will most likely need a business associate agreements implemented are:

- medical billing firms;
- healthcare consultants;
- healthcare lawyers;

- record storage and document destruction companies;
- medical malpractice carriers;
- external audit firms;
- billing collection agencies;
- medical staffing and temporary agencies;
- durable medical equipment vendors;
- medical transcription vendors.

Q5. Under HIPAA, can a hospital release PHI without authorization to another hospital when the patient is being directly transferred?
Yes. PHI can be transferred with the patient or disclosed to the receiving hospital by the transferring hospital. In addition, HIPAA compels healthcare entities to comply with other laws requiring the use or disclosure of PHI. In many instances, state laws may require the disclosure of relevant PHI when a patient is transferred from one hospital to another. These laws would be an additional, but more limited, basis to support disclosure of PHI from a transferring hospital to a receiving hospital.

Q6. A patient's relative sent our department an e-mail to request insurance authorization. The e-mail contains protected health information. Can we respond to the e-mail?
No. First, we need the parent's/guardian's written authorization to share PHI with a third-party. A department member should call the relative to explain that we are not permitted to discuss the information without a written authorization from the parent/guardian. Advise the individual that the parent may call the Medical Record Department at 510-428-3738 to obtain an authorization form.

The brochure *Your Child's Medical Information* contains specific instructions about authorizing release of PHI.

Q7. The newspaper reported that a famous person has come to the hospital for treatment. I am curious if this is true. May I ask around or look for records about this person?
No. We all share a responsibility to protect the privacy of our patients. Accessing patient information to satisfy your curiosity is a breach of patient confidentiality and may result in disciplinary action, including termination of employment or professional relationship with Children's.

PHI Data Elements

1. Names
2. Postal address information, other than town or city, state, and zip code
3. Telephone numbers
4. Fax numbers
5. E-mail addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Bevice identifiers and serial numbers
13. World Wide Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) addresses
15. Biometric identifiers, including voice and fingerprints
16. Full-face photographs and comparable images

*17. All elements of dates (except year) for dates related to an individual

*18. All elements of dates (including year) indicative of age, except an aggregated single category of "90 or older" is permissible

*19. Any other unique identifying number, characteristic, or code

** data elements that are allowed in a Limited Data Set*

PRIVACY, CONFIDENTIALITY & SECURITY OF INFORMATION POLICY

Statement of Policy (HR E07):
Children's values the privacy and confidentiality rights of patients, families, and proprietary hospital information. All employees and affiliates of Children's 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);
- Lanterman-Petris-Short Act (LPS).

APPENDIX II

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 Children's policies that control the way confidential information may be used include, but are not limited to, the following:

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

PRIVACY, CONFIDENTIALITY & SECURITY OF INFORMATION POLICY

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's, its patients, activities and affiliates, in accordance with the law and Children's policy.

I agree to access, use, or disclose confidential information only in the performance of my Children's duties, where required – 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 Children's-related purposes. I will not knowingly discuss any confidential information within the hearing of 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 which is incidentally disclosed to me in the course of my relationship with Children's.

I understand that psychiatric records, drug abuse records, 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 Children's 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 this to Hospital Information Systems and request a new password.

I understand that violation of any of the 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 of 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**
Print Name	**Department**

UCSF Benioff Children's Hospital
Oakland