THE CHILDREN'S MERCY HOSPITAL
ADMINISTRATIVE POLICY

TITLE: Confidentiality
EFFECTIVE: 4/85
REVISION DATE: 3/87, 6/90, 12/95, 10/98, 01/02, 12/03, 1/04, 3/07, 9/09
REVIEWED WITH NO CHANGES:
RETIRED:

PURPOSE:
To outline the responsibilities of Hospital Staff in maintaining and protecting the confidentiality of patient, personnel and Hospital business information that may be gained as part of their job duties.

POLICY:
All patient, personnel and Hospital business information will be held in the strictest confidence and not released without the proper authorization.

DEFINITIONS:
Patient Information: Any clinical, financial or demographic information about a patient whether oral, written, printed, images or electronically stored data.

Hospital Staff: All administrative staff, managers, employees, Medical Staff members, allied health professionals, students and volunteers.

Confidential: Private or personal information that is protected by policy, law, or regulation. Confidential information includes patient, financial, facility and employee information.

Hospital Information: Information including, but not limited to, that information relating to Hospital financial information, business transactions, contracts, payment sources, trademarks, research, patents, strategic plans, marketing strategies, etc.

PROCEDURE:
Written or Printed Information
1. Hospital and patient information should be kept in the appropriate department or patient care area and only viewed to carry out work functions.

2. The physical medical record should not be removed from the area where clinical or other approved work functions are being performed. If the record is to accompany the patient from one location to another, the record must be secured and maintained in the possession of Hospital Staff at all times.

3. When a medical record is viewed, it should be done where other patients or visitors will not have access to see or read the record.

4. Public display of medical information should be limited to non-diagnostic, essential information. In some areas, white boards may be used to coordinate patient care. Such boards may display patients by last OR first names, not both, but may not display any diagnostic information. If patients share the same name, first initial may be used. If patients still cannot be differentiated, a number or other code should be used (e.g., Twin A or Doe #1, etc.).

5. Patient room occupants should be identified in the same manner described above.

6. Students at the Hospital are prohibited from using individually identifiable patient data and other confidential Hospital information obtained within the Hospital for outside education requirements.

7. Any Hospital or patient information that is not to be permanently stored must be appropriately destroyed using the Hospital's shredding vendor.

8. Information and data maintained in any physical medium (paper report, diskette, tape, laptop, PDA, etc.) must be maintained in a secure work location and must not be removed, duplicated or copied except in accordance with a subpoena, court order, or if necessary, testing or treatment of our patient at another facility or without the permission of the employee's supervisor or the appropriate Hospital authority. In such situations, reasonable efforts to protect information should be made such as carrying information in an enclosed case or storage container that conceals the content. In addition, the Hospital's policy on the Security of Remote and Portable Devices must be adhered to at all times.

Electronic Information

1. Accessing or sharing confidential Hospital or identifiable patient information via electronic communication systems must occur in accordance with applicable Hospital policies. Utilizing unsecured electronic communication systems to share confidential information is strictly prohibited except as specifically authorized by Hospital policy. Unsecured electronic communication systems include Internet e-mail and various network systems.

2. Users will be assigned a user name and password for applicable system access and will be responsible for not disclosing or allowing anyone else to use this information.

3. Users will not attempt to gain access to computerized resources other than those they are authorized to receive.

Verbal Communication of Information

1. Hospital Staff shall avoid discussing information with co-workers or any non-employee inside or outside the Hospital, except as such discussion is part of the performance of job duties and the person to whom the information is communicated is authorized and has a need to know that information.

2. The exchange of confidential information should be avoided in public access areas, including elevators, the cafeteria, lobbies, hallways, etc.

3. Due to the limited protection of cellular phone or Vocera conversations, Hospital Staff shall avoid using identifiers in connection with sensitive information when communicating over cellular phones or Vocera.

4. Verbal patient information is not to be given to anyone except to parents or legal guardians, involved health care providers, and authorized child protection and law enforcement staff. Parents or guardians may designate no more than two people, other than themselves, who may receive health information on their child.

5. Patient room number or phone extension inquiries should be directed to the Patient Information Desk, extension 53498, or the Operator. Unless the computer system notes a "confidential" patient or the patient has opted out of the Patient Directory, information regarding the room and extension may be given to the caller. Callers should be reminded that all telephone calls must be placed through the Patient Information Desk or the Hospital Operator.

6. Admissions staff, in accordance with the Confidential Patient Status (Directory and Blackout) policy, should enter information blackout patients and other applicable restrictions into the computer. Thereafter, the patient will either appear as "Confidential" to Hospital Staff with access or have the applicable restrictions noted.

7. The only patient information that may be given to visitors or other relatives is the information available in the Patient Directory.

8. When responding to phone inquiries, Hospital Staff should verify the caller's identity before giving out information. If for any reason the caller's identity is questionable, the staff member has the option of requesting proof of the person's identity, such as asking the person's name, phone number or submission of a fax or request on letterhead. Staff can then return the call to confirm the validity of the caller's request.

9. All media inquiries are to be addressed by the Community Relations department or the Nursing Supervisor.

10. Specific diagnostic tests, results or interpretations may only be given to the parent or guardian by the physician, physician assistant or the advanced practice nurse. A physician, physician assistant or advanced practice nurse may also delegate to a registered nurse the task of sharing this information so long as the physician, physician assistant or advanced practice nurse is aware of critical, abnormal, or unexpected results.

11. Routine patient care information, including frequently monitored laboratory results, may be given to the parent or guardian by the staff nurse, as appropriate.

Responsibilities and Consequences

1. Upon employment and annually, employees will be required to acknowledge in writing (through an acknowledgement statement on the front page of the annual evaluation for, or Attachment A, Confidentiality Agreement) that they have read, understand, and agree to the responsibilities as outlined in this policy and that such responsibilities to protect all types of

confidential information continue even after the staff may terminate their association with the Hospital.

2. Hospital Staff who fails to protect confidential information shall be subject to disciplinary action, up to and including termination of the individual's association with the Hospital, whether that association is employment, educational, contractual, voluntary or participatory and/or action by a licensing board or governmental agency, or an action on behalf of the patient.

3. Concerns regarding potential breaches of confidentiality by any Hospital Staff member should be reported to the Privacy Officer or confidentially through the Compliance Hotline at 816-460-1000.

RELATED POLICIES:
Access to Data and Information
Adoption and Parental Relinquishment Policy
E-mailing of PHI and Other Hospital Information (formerly Electronic Communication to Patients, Parents and Legal Guardians)
Facility Access: Entertainment/Tour
Guidelines for Educational Participation at CMH
Personnel File Access and Use: Notes, (Human Resource Policy Number 405)
Release of Information
Security of Remote and Portable Devices
Photographs, Images, Audio and Video Tapes and Patient Creative Works Use and Release (Formerly: Use and Release of Photographs and Audio and Video Tapes Made For Hospital Purposes)
Visitation (Patient Care Services Policy V-02)

REFERENCES:

WRITTEN BY:
Mikki Massey, Privacy Officer

REVIEWED BY:
Jill Harrelson, Director - Admissions/Medical Records
Jean Ann Breedlove, Chief Information Officer
Theresa Cromwell, Director of Employee Relations
Kim Brown, Vice President – Audit and Compliance
Sally Surridge, Vice President - General Counsel

REVIEW PERIOD:
Per Hospital policy

APPROVED:

Medical Staff Executive Committee	08/05/09
Administrative Council	09/10/09

09/15/2009

Doug Blowey, MD Date
Medical Staff President

09/17/2009

~~Randall L. O'Donnell, PhD~~ Jo Stueve Date
~~President/Chief Executive~~ Officer Executive Vice President

Attachment A

The Children's Mercy Hospital
Confidentiality Agreement

In my affiliation with The Children's Mercy Hospital (Hospital), I understand that:

1. I may have access to confidential information including administrative, affiliate, patient, employee, clinical and financial data which may be in an oral, written or electronic form.
2. I must maintain the confidentiality of all of the information during and after my employment and affiliation. In addition, the confidentiality of the information may be protected by law.
3. The Hospital will investigate instances of unauthorized use of computer resources or unauthorized use or disclosure of confidential information. Unauthorized use or disclosure may result in disciplinary action (including termination of my association with the Hospital, whether that association is employment, educational, contractual, voluntary or participatory) or legal action by the Hospital.

In recognition of the Confidentiality policy, I agree to the following conditions:

1. As a condition of my affiliation with The Hospital, I agree to hold all oral, written and electronic information that I obtain in the course of my affiliation in strict confidence. I understand that if I use or disclose this information without authorization or misuse this information, I may be subject to disciplinary action, (including termination of my association with the Hospital, whether that association is employment, educational, contractual, voluntary or participatory) or legal action by the Hospital.
2. In those cases where I am provided information I will ensure that both the data and the physical medium (paper report, diskette, tape, laptop, PDA, etc.) is maintained in a secure work location and will not be removed, duplicated or copied without the permission of my supervisor or the appropriate Hospital authority.
3. When I am assigned a user name and password for applicable systems I will be responsible for preventing unauthorized use or disclosure of information through misuse of my user name or password. I recognize that my user name and password is equivalent to my signature and must remain under my control at all times. Specifically, I agree that:
    a. I will not disclose my user name or password to anyone or allow anyone else to use my user name or password.
    b. I will not attempt to learn the user name or password of another user.
    c. I will not attempt to obtain access through the computer system to information that I am not authorized to receive.
    d. I will not attempt to access any computerized system resource by using a user name or password not belonging to me.
    e. I will not use my user name or password to access computer resources available to me for any purpose other than for Hospital related projects.
    f. I will not access or attempt to access information after my employment or affiliation with the Hospital.

g. If I know or suspect that the confidentiality of my user name or password or the user name or password of another has been violated, I will immediately notify the Information Systems Security Analyst or the Information Systems Help Line.

4. I understand that failure to report breaches is an ethical violation and may subject me to disciplinary action, (including termination of my association with the Hospital, whether that association is employment, educational, contractual, voluntary or participatory) or legal action by the Hospital.
5. I understand that if I allow any unauthorized person to gain access to computer resources or any confidential information in any form, I may be subject to disciplinary action, (including termination of my association with the Hospital, whether that association is employment, educational, contractual, voluntary or participatory), action by a licensing board or governmental agency, or an action on behalf of the patient and/or legal action by the Hospital.

Signature: _____ Date: ____/____/____

Name (Print): _____

Employee ID#: _____ Department: _____ Position: _____

Supervisor Signature: _____ Date: ____/____/____