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, 8/13, 7/16
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.

LOCATION/SCOPE: The Children’s Mercy Hospital, Children’s Mercy Hospital Kansas and all other locations.

DEPARTMENT RESPONSIBLE FOR POLICY MANAGEMENT & EXECUTION:

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

PROCEDURE:

I. Written or Printed Information

A. Hospital and patient information should be kept in the appropriate department or patient care area and only viewed to carry out work functions.

B. 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.

C. 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.

D. 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 in accordance with the Incidental Uses and Disclosure Policy.

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

G. Any Hospital or patient information that is not to be permanently stored must be appropriately destroyed using the Hospital’s shredding vendor and in accordance with the Record Retention and Management Policy.

H. Information maintained in any physical medium (paper report, etc.) must be maintained in a secure manner and must not be removed, duplicated or copied in accordance with the Release of Information Policy, except in accordance with a subpoena, court order as indicated in the Service of Process, Subpoena, Arrest and Search Warrants and Contact with Attorney Regarding Hospital Business Policy 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. Patient Information removed from a CMH location must be secured in a hard sided locked container as outlined in the Physical Removal and Transport of Protected Health Information and Medical Records Standards.

II. Electronic Information

A. Accessing or sharing confidential Hospital or identifiable patient information via electronic communication systems must occur in accordance with applicable Hospital policies.

B. Electronic information must be handled according to the Data Management Standard. 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.

C. Electronic information in any physical medium (portable media, laptop, or other mobile device) must be secured in accordance with the Media Handling Standard and Mobile Device Procedure.

D. Users will be assigned a user name and password for applicable system access and will be secured as outlined in the Access Management Standard and Password Management Procedure.

E. Users will not attempt to gain access to computerized resources other than those they are authorized to use or receive as part of the employees work duties. Authorized and responsible use of information systems are outlined in the Acceptable Use Standard.
III. Verbal Communication of Information

A. 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.

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

C. Due to the mobile aspect of cellular phone use, Hospital Staff using cellular phones in public areas shall protect patient privacy by avoiding the use of patient identifiers when communicating over cellular phones.

D. 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.

E. In accordance with the Confidential Patient Status Policy, patient room number or phone extension inquiries should be directed to the Patient Information Desk, or the Hospital Operator. Patients have the right to “opt out” of being listed in the Hospital Patient Directory which is managed by the Patient Information Desk or the Operator.

F. Admissions staff, in accordance with the Confidential Patient Status 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.

G. When responding to calls regarding requests for patient information or when leaving messages for families, the Incidental Use and Disclosure Policy guidance must be followed. 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.

H. All media inquiries are to be addressed by the Communication and Marketing Department or the Nursing Supervisor in accordance with the Media Policy.

I. 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. To ensure only designated individuals received such information,
patients and parents should be encouraged to utilize the CMH Patient Portal, MyChildrensMercy, where designated patient information is automatically released.

J. Routine patient care information, including frequently monitored laboratory results, may be given verbally or released to the CMH Patient Portal, MyChildrensMercy by the staff nurse, as appropriate.

IV. Responsibilities and Consequences

A. Upon employment and annually, employees will be required to acknowledge in writing that they have read, understand and agree to abide by the Confidentiality Agreement. The Confidentiality Agreement outlines this policy and that the employee’s responsibility to protect all types of confidential information that continues even after the individual may terminate their association with the Hospital. Confidentiality Agreements may be used for affiliates of the Hospital such as students, observers, vendors, visitors when they may have the opportunity to see patient information as part of their association with the Hospital.

B. 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.

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

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 administrative, affiliate, patient, employee, clinical, Patient Safety Work Product (PSWP), 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, Patient Safety Work Product (PSWP) etc.
REQUESTS FOR DEVIATION FROM POLICY: Requests for deviation from this policy will be directed to the Administrative Council Sponsor for this policy or the Administrator on Call.

RELATED POLICIES:
Acceptable Use Standard
Access to Data and Information
Confidential Patient Status Policy
Data Management Standard
Incidental Uses and Disclosure Policy
Media Handling Standard (Information Security)
Media Policy
Mobile Device Procedure
Password Management Procedure
Personnel File Access and Use: Notes, (Human Resource Policy Number 405)
Record Retention and Management Policy
Release of Information
Service of Process, Subpoena, Arrest and Search Warrants and Contact with Attorney Regarding Hospital Business Policy Transport of Protected Health Information and Medical Records Standards

RELATED FORMS:
Confidentiality Agreement

REFERENCES:

REGULATIONS:

KEYWORD SEARCH: Confidentiality, PHI, Confidential Patient, Black Out, Hotline, CMH Patient Portal, My Children’s Mercy Portal

POLICY CONTENT OWNER:
Mikki Massey, Privacy Officer

ADMINISTRATIVE COUNCIL SPONSOR:
Kim Brown, VP, Audit & Compliance

REVIEWED BY:
Jill Harrelson, Director - Health Information Management
David Chou, Chief Information Officer
Lonna Anderson, Director of Employee Relations
Laurie Ellison, Chief Marketing Officer
Renee Duvall, Information Systems
Amy Crawford, Director, Admissions
MaLiz Denk, Deputy General Counsel & Senior Director of Risk Management
Shelli Crocker, Information Security Officer
Allison Gardner, Senior Director, Ambulatory - Primary Care Specialties/Contact Center

REVIEW PERIOD:
3 years

COMMITTEE REVIEW & APPROVAL:

Administrative Council 7/21/2016

FINAL APPROVAL:

[Signature]
Randall L. O’Donnell, Ph.D. Date
President & Chief Executive Officer 9/27/2016