THE CHILDREN'S MERCY HOSPITAL
ADMINISTRATIVE POLICIES MANUAL

TITLE: Confidentiality of Information Policy
EFFECTIVE: 04/1985
REVISION DATE: 03/1987, 06/1990, 12/1995, 10/1998, 01/2002, 12/2003, 01/2004, 03/2007, 09/2009, 08/2013, 07/2016, 06/2020
REVIEWED WITH NO CHANGES:
RETIRED:

PURPOSE:
To provide standards that preserve confidentiality, integrity and availability of Confidential Information.

LOCATION/SCOPE: The Children's Mercy Hospital (the "Hospital") and its Affiliates; the term "Affiliates" shall refer exclusively to entities or organizations with respect to which the Hospital possesses (a) 100% of the legal or beneficial ownership interests, and (b) the unrestricted power to appoint all members of the governing body (board of directors or comparable governing body). "Unrestricted power" means the power to elect or appoint such members without any limitations (such as a requirement to appoint members from a list of candidates submitted by another party). This policy applies to all Hospital Staff.

DEPARTMENT RESPONSIBLE FOR POLICY MANAGEMENT & EXECUTION:
Corporate Compliance

POLICY:
All Hospital Staff must preserve, protect and maintain confidentiality of the Confidential Information. Unless otherwise specifically permitted under this policy, Hospital Staff shall not use or disclose Confidential Information without prior authorization from the Hospital. This policy is not intended to restrict employees' communications or actions that are protected or required by state or federal law. Any Hospital Staff who is unsure whether information should be kept confidential should consult with the Hospital Staff's supervisor before disclosing the information or taking any other action.

PROCEDURE:

I. General

A. **Protocols**. Hospital Staff must treat all Confidential Information as strictly confidential. To maintain the confidentiality of Confidential Information, all Hospital Staff must follow these protocols, except as otherwise provided in this policy:

- Hospital Staff should not access or use any Confidential Information to which the Hospital has not provided the staff access or authorization to use.

- Hospital Staff should not directly or indirectly disclose, publish, communicate, or make available Confidential Information to any entity or person that does not have a need or the authority to know and use the Confidential Information, except as required for the Hospital Staff to perform authorized job duties or otherwise permitted by this policy.
- If a Hospital Staff's authorized job duties require sharing Confidential Information with a third party, the Hospital Staff must not do so until the Hospital and the third party enter into a confidential confidentiality agreement.
- Hospital Staff may not remove Confidential Information from the workplace unless specifically approved in writing by the Hospital Staff's supervisor to perform the Hospital Staff's authorized job duties or otherwise permitted by Hospital policy.
- Departing Hospital Staff must return any Confidential Information in the Hospital Staff's possession to the Hospital on termination of relationship with the Hospital.
- Concerns regarding potential breaches of confidentiality by any Hospital Staff must be reported to the Privacy Officer or confidentially through the Corporate Compliance Hotline at 816-460-1000.

B. **Disclosure of Trade Secrets**. As provided for by the Economic Espionage Act of 1996, as amended by the Defend Trade Secrets Act of 2016, employees will not be held criminally or civilly liable under any federal or state trade secret law for any disclosure of a trade secret that is made:

   i. in confidence to a federal, state or local government official, either directly or indirectly, or to an attorney, and solely for the purpose of reporting or investigating a suspected violation of law; or
   ii. in a complaint or other document that is filed under seal in a lawsuit or other proceeding.

   If an employee files a lawsuit for retaliation by the Hospital for reporting a suspected violation of law, the employee may disclose the Hospital's trade secrets to the employee's attorney and use the trade secret information in the court proceeding if the employee:

   i. files any document containing the trade secret under seal; and
   ii. does not disclose the trade secret, except pursuant to court order.

C. **Confidentiality Agreements**.

   i. Upon employment and annually, employees will be required to acknowledge in writing that they have read, understand and agree to abide by the Hospital Confidentiality Agreement. The Hospital Staff Member Confidentiality Agreement outlines this policy and the employee's responsibility to protect all types of Confidential Information, which continues even after the employee separates from the Hospital.
   ii. Certain employees may have an employment agreement with the Hospital that contains terms of confidentiality. In the event there is any inconsistency between this policy and an employee's individual confidentiality agreement, the terms of the confidentiality agreement shall govern.

iii. The Hospital also requires third parties, including independent contractors, to sign a confidentiality agreement before receiving any Confidential Information. Employees must help ensure the protection of Confidential Information by abiding by this requirement when communicating or sharing information with a third party with whom the Hospital is doing business.

II. Written or Printed Information

A. Confidential Information must be kept in the appropriate department or patient care area and only viewed to carry out required work functions. Exception: Confidential Information disseminated internally via hand delivery or via internal mail which should be marked as "Confidential."

B. A physical medical record should not be removed from the area where clinical or other approved work functions are being performed. If a physical 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. Written or printed medical records removed from a Hospital location must be secured as outlined in the Physical Removal and Transport of Protected Health Information and Medical Records Standards.

C. When written or printed Confidential Information is viewed, it should be done where others not authorized to view the information will not have access to the Confidential Information.

D. Public display of written or printed medical records 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 Disclosures of Protected Health Information (PHI) Standard and the Uses and Disclosures of Protected Health Information (PHI) Standard.

E. Patient room occupants should be identified in accordance with the Incidental Uses and Disclosures of Protected Health Information (PHI) Standard.

F. Any written or printed Confidential Information which will not be permanently stored must be appropriately destroyed using the Hospital's shredding vendor, subject to and in accordance with the Record Retention and Management Policy.

III. Electronic Information

A. Accessing or sharing Confidential Information via electronic communication systems must occur in accordance with all Hospital policies, including the Electronic Communication of PHI 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 email and may include some networked systems.

B. Hospital Staff may be assigned a user name and password for applicable system access and which such Hospital Staff member must secure as outlined in the Password Management Procedure.

C. Hospital Staff will not attempt to gain access to computerized resources other than those they are authorized to use or access as part of such staff's work duties.

D. When electronic Confidential Information is accessed, it should be done where those not authorized to view the information will not have access to such Confidential Information.

IV. Oral Communication of Information

A. Hospital Staff are prohibited from discussing Confidential Information with or in the presence of co-workers or any non-Hospital Staff inside or outside the Hospital, except as such discussion is part of the performance of job duties and the person receiving the information is authorized and has a need to know that information. Furthermore, with respect to PHI, the Uses and Disclosures of Protected Health Information (PHI) Standard and the Incidental Uses and Disclosures of Protected Health Information (PHI) Standard should be followed.

B. The disclosure of Confidential Information should be avoided in public access areas, including elevators, the cafeteria, lobbies, hallways, and so on.

C. Oral communication of PHI is not to be given to anyone except to patients, parents or legal guardians, involved health care providers, people who have received Authorization, and authorized child protection and law enforcement staff.

D. In accordance with the Restricting Access to Inpatients and/or their Patient Information standard, patient room number or phone extension inquiries should be directed to the Patient Information Desk (aka Patient Access), 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 Hospital Operator. Hospital Staff should enter information for 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.

E. When responding to calls regarding requests for PHI or when leaving messages for families, the guidance in the Incidental Uses and Disclosures of Protected Health Information (PHI) Standard must be followed.

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

G. Specific diagnostic tests, results or interpretations may be given only to the parent, guardian or patient (as appropriate) 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 receive such information, patients and parents should be encouraged to use the Hospital's patient portal, MyChildrensMercy Patient Portal.

H. Routine patient care information, including frequently monitored laboratory results, may be given orally or released to the Hospital's patient portal, MyChildrensMercy Patient Portal, by the staff nurse, as appropriate.

V. Use of Confidential Information (applicable to all Confidential Information regardless of its format)

A. Access and use of Confidential Information should be done in accordance with the Access to Data and Information Policy and the Uses and Disclosures of Protected Health Information (PHI) Standard.

B. Students at the Hospital are prohibited from using or disclosing Confidential Information obtained within the Hospital for external (non-Hospital) education requirements.

C. Confidential Information maintained in any physical medium (paper report, diskette, tape, laptop, personal data assistant) must be maintained in a secure manner and must not be removed, duplicated or copied except in accordance with the Release of Information Policy, and except in accordance with a subpoena, court order as indicated in the Service of Process, Subpoenas, Arrest and Search Warrants and Contact with Attorneys Regarding Hospital Business Policy or if necessary, testing or treatment of our patient at another facility or without the permission of the Hospital Staff's supervisor or the appropriate Hospital authority. PHI removed from a Hospital location must be secured in a hard-sided locked container as further outlined in the Physical Removal and Transport of Protected Health Information and Medical Records Standards.

VI. Violations

A. 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.

B. Hospital Staff who fail 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.

DEFINITIONS:

Confidential Information includes, but is not limited to, all information belonging to the Hospital and not generally known to the public, in spoken, printed, electronic or any other form or medium, which was obtained from the Hospital, or which was learned, discovered, developed, conceived, originated, or prepared by Hospital Staff in the scope and course of employment, relating to: business processes, practices, methods, policies, plans, research, operations, services, strategies, techniques, agreements, contracts, transactions, potential transactions, negotiations, know-how, trade secrets, applications, operating systems, software design, supplier/vendor information, financial information, accounting information, legal information, marketing information, pricing information, credit information, payroll information, internal controls, security procedures, revenue, costs, client/customer information or of any other person or entity that has entrusted information to Hospital in confidence. Confidential Information also includes other information that is marked or otherwise identified as confidential or proprietary by or on behalf of the Hospital, and Hospital information that would otherwise appear to a reasonable person to be confidential or proprietary in the context and circumstances in which the information is known or used, other than employees' terms and conditions of employment.

Hospital Staff means all Hospital employees, Board members, executives, employed and non-employed health care professionals, health care professionals with clinical privileges, contract staff, volunteers, students and persons conducting research on behalf of the Hospital.

Note: See the Glossary for HIPAA Policies for additional applicable definitions of terms.

REQUESTS FOR GUIDANCE REGARDING POLICY:

Requests for guidance regarding this policy will be directed to the Administrative Council sponsor.

BUSINESS CONTINUITY AND DISASTER (BCD) PLAN:

MEASUREMENTS/METRICS:

RECOURSE FOR NON-COMPLIANCE:

Non-compliance will be addressed in accordance with the Conduct and Corrective Action Policy.

RELATED POLICIES:

Access to Data and Information Policy
Electronic Communication of PHI Standard
Employee File Access and Use Policy
Incidental Uses and Disclosures of Protected Health Information (PHI) Standard
Media Policy

Password Management Procedure
Physical Removal and Transport of Protected Health Information and Medical Records Standards
Record Retention and Management Policy
Release of Information Policy
Restricting Access to Inpatients and/or their Patient Information
Service of Process, Subpoenas, Arrest and Search Warrants and Contact with Attorneys Regarding Hospital Business Policy
Uses and Disclosures of Protected Health Information (PHI) Standard

RELATED FORMS:

Hospital Staff Member Confidentiality Agreement
Notice of Privacy Practices

REFERENCES:

MyChildrensMercy Patient Portal

REGULATIONS:

KEYWORD SEARCH:

confidentiality, PHI, confidential patient, black out, hotline, patient portal, my children's mercy portal, patient portal

POLICY CONTENT OWNER:

Mikki Massey, Privacy Officer, Corporate Compliance

ADMINISTRATIVE COUNCIL SPONSOR:

Kim Brown, VP, Audit and Compliance

REVIEW PERIOD:

Three (3) years

REVIEWED BY:

Lonna Anderson, Sr. Director, Employee Relations and HR Compliance
Shelli Crocker, Information Security Compliance Officer, Corporate Compliance
Audrey Kennedy, Director, Clinical Safety
Irfan Shaikh, Sr. Director, Revenue Cycle
Natalia Sierra, Director, Revenue Cycle (Interim)

LEADERSHIP REVIEW:

Kim Brown, VP, Audit and Compliance
Stacy Doyle, Sr. VP, Ambulatory and Physician Practice Operations
Laurie Ellison, Sr. VP, Chief Marketing Officer

Beau Gostomsky, VP, Revenue Cycle
Cheri Hunt, Sr. VP, Patient Care Services and Chief Nursing Officer
Office of General Counsel/Risk Management

FINAL APPROVAL:

Paul Kempinski, President, Chief Executive Officer