Policy Number:	**8.00**	**Original Date Issued:**	June 25, 2001
Section:	Information Management	**Date Reviewed:**	April 12, 2010
Title:	Confidentiality of Information	**Date Revised:**	April 12, 2010
Regulatory Agency:	**HIPAA, ORS, DHHS, OSHA, TJC**		

Now includes information from 7-02 Faxing Patient Health Information; 8-01 Electronic File Naming Policy 8-04 Information Security and Confidentiality which were deleted.

I. POLICY:

Children's Healthcare of Atlanta (Children's) requires Confidentiality of Information primarily for the purpose of protecting the confidentiality of patients and/or Hospital/System business interest(s). Information, records or material, including information stored electronically, concerning patients and Hospital/System business is confidential and may not be used, released or discussed with anyone outside Children's or with other employees without prior authorization from Administration.

II. PROCEDURE

APPROPRIATE USE AND ACCESS TO INFORMATION: There are an abundance of needs and legitimate reasons for sensitive information to be accessed, reviewed or reproduced. Appropriate uses include, but not limited to:

- Patient care
- Education
- Customer Service
- Public Health in accordance with legal regulations
- Judicial proceedings
- Law enforcement
- Research and clinical, scientific, and other professional publications
- Billing
- Marketing
- Managed care contracting
- Medical and managerial peer review and medical credentialing
- Administrative purposes
- Corporate financial analysis, including planning and forecasting
- Quality assurance and quality improvement initiatives
- Physician practice reporting
- Reporting purposes mandated by legal, regulatory, or other database reporting

All patients at Children's will be informed of the need to use patient information for legitimate patient care needs and business processes in accordance with strict rules governing patient

privacy and confidentiality. All patients will be asked to sign a statement acknowledging receipt of a privacy notification.

INAPPROPRIATE USE AND ACCESS TO INFORMATION: Access to patient and organizational data is appropriate if access is within the scope of and required for the performance of the requestor's job duties and/or responsibilities on behalf of the patient or organization. Access to and/or distribution of patient and/or organizational information for inquisitive, illicit, or illegal use will not be tolerated and is in direct violation of this policy. Violators will be subject to appropriate administrative disciplinary actions and/or potential civil and/or criminal litigation based upon applicable local, state and federal laws. Examples of inappropriate use include but are not limited to:

- Accessing information without a legitimate business need
- Knowingly and deliberately falsifying information in the non-test environment, for whatever purpose
- Using data for purposes other than were intended
- Misrepresenting reasons for necessary reviews of information
- Providing others with data who are not approved or do not have a legitimate business need
- Using information for personal or financial gain by gathering or disseminating it without authorization from those affected
- Using data without going through the proper procedures to obtain it
- Releasing or using data that is incomplete or inaccurate
- Publishing (includes the internet and any other mass or social media) information via a medium whose security has not been approved by Children's as appropriate for the transmission of information about Children's or the patients of Children's

ACCESS TO INFORMATION DOES NOT IMPLY AUTHORIZATION TO ACCESS INFORMATION: Current technology provides access to many kinds of information by physicians, employees, and others. The ability to access data does not in itself create an inherent right, clinical or business, to obtain that information or disperse it. **EMAIL, PRINTING, FAXING and INTERNET TRANSMISSIONS**: Precautions should be taken in the use of internal and/or external electronic mail systems or faxing for the distribution of information of a potentially confidential nature.

COMPLIANCE AND MONITORING: Employees, trainees, students, medical staff, allied health personnel and residents shall sign a Security and Confidentiality Agreement (Attachment A) at the time of orientation or rotation through Children's. Contracts with third-party vendors who will have access to patient information will contain provisions that commit these vendors and their employees to the HIPAA standards of confidentiality and privacy of patient information.

Signed agreements will be kept in the respective employee files in Human Resources and a copy provided to the Department Manager. Failure to sign the agreement does not exempt the employee, staff member or vendor from meeting the previous expectations. Medical staff and

resident agreements will be kept and maintained by Medical Staff Services. Each employee's manager and Medical Staff Services are responsible for consent completion.
Routine random audits will be conducted on the system to measure compliance with established policies and appropriate system use. Audits may be conducted relative to all users, systems and timeframes. Audit frequency should reflect consideration for the sensitivity of the data and the potential likelihood of misuse and abuse.
Results of audits will be reported to the appropriate departments and leadership as needed. Violators will be reported to Human Resources, Quality Management, Medical Staff Services, Department Managers and Information Systems & Technology immediately for appropriate actions and recommendations. It is the responsibility of those departments to ensure that appropriate actions are taken.

III. AFFECTED TYPES OF INFORMATION

A. **Patient Information**: The patient's health record is the property of Children's whether it is the original paper record stored in Medical Records or archived via electronic media and is carefully maintained to service the patient, the health care providers and Children's in accordance with legal, accrediting and regulatory agency requirements. All patient care information shall be regarded as confidential and may be used or communicated only in compliance with Children's privacy policies.

B. **Children's Hospital Information:** Information regarding Hospital business, pricing, information systems, employee problems and disciplinary actions are considered confidential and should only be discussed with those individuals who have a job related "need to know."

C. **Children's Hospital Documents:** Hospital documents are considered Children's property and their removal can constitute theft. Hospital documents and electronic files may not be removed from the premises without written authorization from the employee's supervisor. All hospital property and documents should be returned at the time of an employee's termination of employment.

D. **Personnel Material:** Personnel files and similar employment documents are Children's property and may not be removed or copied by employees. This does not prohibit current employees from reviewing their files, receiving copies of evaluations, counseling or other documents given to them by their supervisor necessary for their ongoing performance. Former employees are not allowed access to their files. All salary, meritincreases, benefit information and all other materials related employment are also considered confidential and should not be discussed with other employees. Permanent and departmental copies of personnel files are to be safeguarded from theft, unauthorized use and damage by providing a secured storage area.

E. **Employee Medical Information:** The employee's health record is the property of Children's and is carefully maintained in order to service the employee, employee health care providers and the Children's in accordance with legal, accrediting and regulatory agency requirements. This information is regarded as confidential and is available to the employee health care provider, the employee or his designee. Information regarding work-related injury or illness and pre and post exposure testing will be made available to an OSHA inspector upon request. Information about an employee, i.e., test results, will not be given over the telephone and requests for information are to be in person or in writing.

F. **Protected Health Information:**
Any health information provided by an employee to a supervisor is Protected Health Information (PHI). If a written record of the information is created, it must be submitted and stored in the Employee Health department, in the employee's medical record. Any PHI related to the employee and included in the employee health record is considered privileged. Due to the confidential nature of the information, only minimum, necessary privileged information can be disclosed upon receipt of written authorization from the employee. (Please refer to the Employee Medical Records policy #9.29)

G. **Medical Staff Credentialing Materials:** Medical staff credentialing files are Children's property and may not be removed from the Medical Staff Credentialing Department. Physicians are required to sign a release of information before any credentialing information is shared with another provider organization.

H. **Confidentiality Statement:** Employees are required to sign a Confidentiality Agreement (See Attached) at General Orientation.

I. **Discipline:** Non-compliance or breaches of these confidentiality requirements may result in disciplinary action, up to and including termination. In addition, failure to respect the confidentiality of these types of documents and information can be a violation of law.

EMPLOYEE CONFIDENTIALITY STATEMENT

I understand and agree to abide by the "Confidentiality of Information," Children's Policy, Number 8.00, and behave in a professional, ethical manner at all times, regarding patient and hospital/system business confidentiality. I understand that misconduct and/or breaches of confidentiality may be grounds for disciplinary action up to and including termination of employment.

Printed Name	Employee ID #
Signature	Date