Policy Number:	**TBD**	**Original Date Issued:**	**10/3/2013**
Section:	**Data Use**	**Date Reviewed:**	**10/3/2013**
Title:	**Appropriate Data Use**	**Date Revised:**	**10/3/2013**
Regulatory Agency:	**HIPAA**		

I. **PURPOSE**:

This policy defines Children's Healthcare of Atlanta and System Affiliates' (collectively, Children's) commitment to implementing an Appropriate Date Use framework and associated measures that sufficiently provide guidance for reducing the risks to the distribution, sharing and use Children's confidential and sensitive data.

SCOPE:

This policy applies to all users of Children's data that is retrieved from application or system data repositories. The policy reflects a documented process regarding limitations and/or protection requirements for Children's confidential and sensitive information. This policy is governed by Business Intelligence Governance and Steering committee and sub-committees and is designed to comply in conjunction with the Information Security policies and reflects consistent requirements for the protection of Children's sensitive and confidential information.

II. DEFINITIONS:

A. **Data Requester:** An individual, employed by Children's or not employed by Children's who requests data. If a data requester is not a member of Children's staff, a Data Sponsor is required.

B. **Data Sponsor:** A Children's employee who "sponsors" the request for data on-behalf of a non-children's data requester.

C. **Data Recipient:** The individual who receives data. This person can be employed or not employed by Children's.

D. **Children's Data Recipients:** Recipients of data who are employees of Children's are legally covered and bound by the internal policies of Children's.

E. **Non-Children's Data Recipient:** Recipients of data who are not employees of Children's.

F. **Business Intelligence Governance and Steering (BIGS):** The governing body responsible for establishing this policy.

G. **Data Steward Councils:** Data subject teams established by the BIGS council that are responsible for supporting and oversight for privacy and appropriate use of data subject areas.

H. **Data Authority:** The data subject area authority on a Data Steward Council, who is responsible for establishing guidelines for appropriate access and approval of data use.

III. POLICY:

This policy acknowledges that all information collected or produced by Children's is the sole property of Children's Healthcare of Atlanta. Information concerning patients, employees, medical staff, quality, outcomes, financial, 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 and by the appropriate data steward councils identified in this policy. This policy protects the property rights by addressing definition, responsibility, control, and use of sensitive information shared by Children's internally and externally.

A. **APPROPRIATE USE:** There are multiple 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

B. **INAPPROPRIATE USE:** Access to data is inappropriate if access is not within the scope of and required for the performance of the requestor's job duties and/or responsibilities on behalf the organization. Access to and/or distribution of patient and/or organizational information for inquisitive, illicit, or illegal use 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 tended
- 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
- Publishing without going through proper procedures to obtain approval for publication

C. **ACCESS TO 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 distribution.

1. Access to information through an established application is granted through the application rights and polices used to create the data.

2. Request for access to information and data sets through alternative data reporting, data visualization, data extraction, or data technology must be approved through the REQUEST FOR ACCESS TO INFORMATION AND DATA SETS section of this policy.

D. REQUESTS FOR ACCESS TO INFORMATION AND DATA SETS

1. Children's will establish a central process for requesting and monitoring compliance for data requests.

2. The Business Intelligence Governance and Steering (BIGS) council is responsible for governing the process for data access, retrieval, and governance.

3. BIGS will form appropriate Data Steward Councils responsible for

    a) granting access to data consistent with the classification of the data, role(s) and responsibilities of the user, and appropriate use;

    b) providing oversight for privacy and appropriate use of data subject areas.

E. DATA CATEGORIES AND STEWARDSHIP

1. Data Categories are high level classifications of the Children's data that require specific security or privacy considerations. Data categories represent data that require unique access requirements as described above. Each data-category is assigned to a Data Steward Council.

2. The Data Steward Council is responsible for supporting and oversight for privacy and appropriate use of data subject areas. The Data Steward Council follows the guidelines established by the Data Authority.

3. The Data Authority is responsible for establishing the guidelines for appropriate access and approval of data use.

Data Category	Data Steward Council	Data Authority
Patient Information	BIGS – Clinical Subgroup	Privacy Officer
Hospital Financial and Business Operations Information	BIGS – Finance Subgroup	Clinical CFO
Employee and Personnel Data	BIGS – HR Subgroup	Director, HR

Data Category	Data Steward Council	Data Authority
Medical Staff Credentialing Materials	Medical Staff Services	Director - Medical Staff
Quality	BIGS – Clinical Subgroup	Medical Director, CMIO
Outcomes	BIGS – Clinical Subgroup	Director - Outcomes
All Other Data	Business Intelligence Governance & Steering	BIGS Chair

F. DATA USE COMPLIANCE AND MONITORING

1. Children's Data Recipient Compliance

    a. The procedure for requesting access shall be governed by the REQUESTS FOR ACCESS TO INFORMATION AND DATA SETS section of this policy.

    b. Children's employees, staff personnel who request data shall sign and abide by the requirements of an **Appropriate Data Use Acknowledgment – Data Recipient** (Appendix A) with each new data request.

    c . Signed acknowledgements will be kept retained and kept on file with original data request document maintained by the central data request repository managed by IS&T Business Intelligence.

2. Non-Children's Data Recipient Compliance

    a. The procedure for requesting access shall be governed by the REQUESTS FOR ACCESS TO INFORMATION AND DATA SETS section of this policy.

    b. All non-Children's data requesters must obtain sponsorship from a qualified Children's staff member.

    c. Children's sponsors who requests data shall sign and abide by the requirements an **Appropriate Data Use Acknowledgment – Data Sponsor** (Appendix B) with each new data request. Signed acknowledgements will be kept retained and kept on file with original data request document maintained by the central data request repository.

    d. Non-Children's business associates or individuals that request access to data are

required to demonstrate a legitimate business relationship with Children's Healthcare of Atlanta as demonstrated through a current and signed **Business Associates Agreement.**

e. Non-Children's business associates or individuals who will have access to sensitive shall sign and abide by the requirements of a **Data Use Agreement - For Disclosure of a Limited Data Sets** (Appendix C).

G. EXCEPTIONS:

Exceptions to this Policy must be approved in writing, in accordance with the *Appropriate Data Use Exception procedure*. New exception requests will be reviewed in accordance with the *Appropriate Data Use Exception procedure*. Any approved policy exception will be reviewed periodically for appropriateness, and may be revoked at any time by notifying appropriate personnel.

H. POLICY REVIEW:

This policy will be reviewed and updated annually, as required by law or relevant regulation, or as needed. During review, the policy will be evaluated to determine: 1) effectiveness in complying with key regulations such as the HIPAA Security Rule and 2) effectiveness of meeting Children's evolving operational needs.

In accordance with the Code of Federal Regulations, 45 C.F.R. 164.306(b)(2)(i), all iterations of this Policy will be retained for a minimum of 6 years.

I. POLICY AUTHORITY/ENFORCEMENT:

The Business Intelligence Governance and Steering council has general responsibility for implementation of this policy.

Violations of this policy may result in suspension or loss of the violator's use privileges, with respect to Children's Resources, and/or disciplinary action in accordance with the Children's *Sanction Policy #x-xxx*. Additional civil, criminal and equitable remedies may apply. Access privileges may be restored only after consultation between the designated Information Security Officer and Children's Management and/or Children's Senior Management personnel.

Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor; or via the established Compliance reporting methods found on the *Compliance Department Site.*

APPROVED BY:

Appendix A

Children's Healthcare of Atlanta Appropriate Data Use Agreement – Data Recipient

STATEMENT OF POLICY

It is the legal and ethical responsibility of all Children's Healthcare of Atlanta and System Affiliates (collectively, Children's) Information Users to use personal and confidential patient, employee and business information (referred here collectively as "confidential information") in accordance with the law, Children's policies, including the Code of Conduct , and to preserve and protect the information that you have access to.

Children's policies that control the way confidential information may be used are located on Careforce Connection. It is your responsibility to review and assure your compliance with these policies and requirements.

Confidential information includes Patient Information, Protected Health Information, Financial Information, Hospital Business/Operations Information, Employee and Personnel Information, Medical Staff Credentialing Information, Quality and Outcomes Information, Education Information, etc. Please review Children's Policy 8.00 "Confidentiality of Information" for types of confidential information and appropriate use.

Laws controlling the use, disclosure and maintenance of confidential information regarding patients include, but are not limited to, the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). This and other laws apply whether the information is maintained in electronic or any other form, and whether the information is used or disclosed orally or in writing. It is your responsibility to review and assure your compliance with these requirements.

ACKNOWLEDGMENT OF RESPONSIBILITY

I understand and acknowledge that:

It is my legal and ethical responsibility as an authorized user to preserve and protect the privacy, confidentiality and security of <u>all</u> confidential information collected, created , derived, or maintained by Children's in accordance with the law and Children's policy.

It is my legal and ethical responsibility to ensure that all confidential information I access is required for the particular purpose for which I am accessing, disclosing or using it.

I agree to access, use or disclose only the confidential information needed to perform my job duties, when required or permitted by law, and to disclose information only to persons who have the right to receive that information.

I agree to protect the confidentiality of any confidential information which is disclosed to me in the course of my relationship with Children's.

I agree that Children's disclosed Protected Health Information is limited in scope to the minimum Protected Health Information necessary to accomplish my purpose.

I have read and agree to abide by Children's Information Security Risk Management Policy, procedures relating to electronic communication of data of Children's Information Technology Acceptable Use Policy, proper handling and disposal of PHI information including Children's Secure Disposal, and Information Security Sanction Policy.

I understand that misconduct and/or breaches of Children's policies and procedures related to confidential information or any state or federal laws or regulations governing confidential information or violation of confidentiality may subject me to legal and/or disciplinary action up to and including immediate termination from my employment/professional relationship with Children's, fines and imprisonment. Violation of Local, State or Federal statutes may carry the additional consequence of prosecution under the law. In addition I understand that I may be personally liable for harm resulting from my breach of this Agreement.

I have read and agree to abide by the above STATEMENT OF POLICY AND ACKNOWLEDGEMENT OF RESPONSIBILITY.

Project/Report/Data Request title _____

_____

Print Name

_____

Signature

_____

Date

Appendix B

Children's Healthcare of Atlanta Appropriate Data Use Agreement – Data Sponsor

STATEMENT OF POLICY

It is the legal and ethical responsibility of all Children's Healthcare of Atlanta and System Affiliates (collectively, Children's) Information Users to use personal and confidential patient, employee and business information (referred here collectively as "confidential information") in accordance with the law, Children's policies, including the Code of Conduct , and to preserve and protect the information that you have access to.

Children's policies that control the way confidential information may be used are located on Careforce Connection. It is your responsibility to review and assure your compliance with these policies and requirements.

Confidential information includes Patient Information, Protected Health Information, Financial Information, Hospital Business/Operations Information, Employee and Personnel Information, Medical Staff Credentialing Information, Quality and Outcomes Information, Education Information, etc. Please review Children's Policy 8.00 "Confidentiality of Information" for types of confidential information and appropriate use.

Laws controlling the use, disclosure and maintenance of confidential information regarding patients include, but are not limited to, the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). This and other laws apply whether the information is maintained in electronic or any other form, and whether the information is used or disclosed orally or in writing. It is your responsibility to review and assure your compliance with these requirements.

ACKNOWLEDGMENT OF RESPONSIBILITY

I understand and acknowledge that:

It is my legal and ethical responsibility as an authorized sponsor of the data request to preserve and protect the privacy, confidentiality and security of <u>all</u> confidential information collected, created , derived, or maintained by Children's in accordance with the law and Children's policy.

It is my legal and ethical responsibility to ensure that all confidential information for which I am sponsoring access is required for the particular purpose for which the data recipient is accessing, disclosing or using it.

I agree that the data recipient's access, use or disclosure of confidential information is needed to perform the data recipient's job duties.

I agree that Children's disclosed Protected Health Information is limited in scope to the minimum Protected Health Information necessary to accomplish the data recipient's purpose.

I have read and agree to abide by Children's Information Security Risk Management Policy, procedures relating to electronic communication of data of Children's Information Technology Acceptable Use Policy, proper handling and disposal of PHI information including Children's Secure Disposal, and Information Security Sanction Policy.

I understand that misconduct and/or breaches of Children's policies and procedures related to confidential information or any state or federal laws or regulations governing confidential information or violation of confidentiality may subject me to legal and/or disciplinary action up to and including immediate termination from my employment/professional relationship with Children's, fines and imprisonment. Violation of Local, State or Federal statutes may carry the additional consequence of prosecution under the law. In addition I understand that I may be personally liable for harm resulting from my breach of this Agreement.

Name of Data Recipient you are sponsoring _____

Project/Report/Data Request title _____

I have read and agree to abide by the above STATEMENT OF POLICY AND ACKNOWLEDGEMENT OF RESPONSIBILITY.

_____

Print Name

_____

Signature

_____

Date

Exhibit C

Children's Healthcare of Atlanta Appropriate Data Use Agreement – Non-CHOA Data Recipient

This Data Use Agreement (this "Agreement") is entered into this _____day of _____2011("Effective Date") between _____ ("Data Recipient") and Children's Healthcare of Atlanta, Inc. and its affiliated corporations, a Georgia nonprofit corporation ("Children's") for purposes of compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

RECITALS

A. Data Recipient will receive a Limited Data Set for the purpose of research project _____; and

B. Children's agrees to disclose a Limited Data Set (See attachment A) to Data Recipient for use by Data Recipient in performing the Activities described in the Project; and

D. Data Recipient agrees to limit its use of the Limited Data Set and protect the Limited Data Set according to the terms and conditions of this Agreement, and all applicable requirements of HIPAA and the Privacy Rule (as defined below), as amended from time to time.

NOW THEREFORE, in consideration of the foregoing and other good and valuable consideration, the parties agree as follows:

1.0 **DEFINITIONS**.

Capitalized terms used but not otherwise defined in this Agreement shall have the same meaning as those terms are defined in the Standards for Privacy of Individually Identifiable Health Information, 45 CFR part 160 and part 164, subparts A and E, as amended (the "Privacy Rule").

2.0 **DISCLOSURE OF LIMITED DATA SET TO DATA RECIPIENT**.

2.1 Scope of Limited Data Set. For purposes of this Agreement, the Limited Data Set may consist of, but is not limited to, the Protected Health Information listed in Attachment A (the "Limited Data Set").

This does not include any identifiers prohibited in the "Limited Data Set Statement and Assurance" (see, 45 CFR 164.514(e)(2)). Scope of Limited Data Set will be limited to the minimum necessary to perform the Activities.

2.2 Disclosure of Limited Data Set. Children's agrees to disclose the Limited Data Set to Data Recipient solely for use by Data Recipient to perform the Project described in A., and Data Recipient agrees that it shall not use the Limited Data Set for any other purpose. Data Recipient further agrees that Data Recipient shall limit access to and the use of the Limited Data Set to individuals who need the Limited Data Set to perform activities related to the Project.

3.0 **OBLIGATIONS OF DATA RECIPIENT**.

3.1. Use of Limited Data Set. Data Recipient (including without limitation its employees, officers, directors, and volunteers) shall not use or disclose the Limited Data Set except as permitted under the terms of this Agreement or as required by law.

3.2 Safeguards Against Misuse of Information. Data Recipient shall use appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as permitted under this Agreement.

3.3 Reporting of Disclosures of Protected Health Information. Data Recipient shall notify Children's of any use or disclosure of the Limited Data Set in violation of this Agreement by Data Recipient, its officers, directors, employees, contractors or agents, or by any third party, within five days of Data Recipient having knowledge of any such violation. Such notice shall be in writing and may be sent by fax or email as outlined in section 8.3 below.

3.4 Use of Data. Any data shared pursuant to this Agreement may be used for research purposes only. In the case of "research involving human subjects," as defined under the "Common Rule" at 45 CFR Part 46 and associated guidance issued by the Office of Human Research Protections (OHRP), appropriate Institutional Review Board (IRB) review and approval must be obtained (including, but not limited to, obtaining an IRB determination that the research is exempt per 45 CFR Part 46.102(d), 102(f), and applicable OHRP Guidance) prior to release of the data.

3.5 No Commercial Use. Data provided pursuant to this agreement shall not be sold, used for marketing purposes, or used in any other manner that shall constitute a commercial use.

3.6 Minimum Necessary Information. Data Recipient represents that Data Recipient's request that Children's disclose Protected Health Information to Data Recipient is limited in scope to the minimum Protected Health Information necessary to accomplish Data Recipient's purpose in connection with the Activities.

3.7 Notice of Request for Data. Data Recipient agrees to notify Children's within five (5) business days of Data Recipient's receipt of any request or subpoena for Protected Health Information relating to this Agreement. Such notice shall be in writing and may be sent by fax or email as outlined in section 8.3 below. To the extent that Children's decides to assume responsibility for challenging the validity of such request, Data Recipient shall cooperate fully with Children's in any such challenge.

4.0 **OWNERSHIP OF INFORMATION**.

Data Recipient acknowledges that, as between Data Recipient and Children's, all Protected Health Information received or developed by Data Recipient in connection with this Agreement shall be and remain the sole property of Children's Healthcare of Atlanta. Notwithstanding the foregoing, Children's acknowledges that the Data Recipient is the sole owner of the aggregate database created by Data Recipient.

5.0 **TERM AND TERMINATION**.

5.1 Term. The term of this Agreement shall commence as of the Effective Date set forth above and shall terminate when Data Recipient no longer performs the Activities on behalf of Children's and all of the Protected Health Information provided by Children's to Data Recipient, or created or received by Data Recipient on behalf of Children's, is destroyed or returned to Children's, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

5.2 Termination for Cause. Upon Children's knowledge of a material breach by Data Recipient, Children's shall:

(a) Provide Data Recipient with written notice of the breach and an opportunity to cure the breach within thirty (30) calendar days of receipt of such notice. Data Recipient shall immediately take steps to mitigate the breach and shall cure the breach within the thirty (30) day notice period. If Data Recipient fails to mitigate and cure the breach within the notice period Children's may immediately terminate this Agreement; or

(b) Immediately terminate this Agreement (without opportunity to cure) if Children's determines, in Children's sole discretion, that Data Recipient has breached a material term of this Agreement.

5.3 Effect of Termination. Upon termination of this Agreement, Data Recipient shall, upon the request of Children's, either return or destroy all Protected Health Information received from Children's, or created or received by Data Recipient on behalf of Children's, and thereafter Data Recipient shall not retain any copies of such Protected Health Information. Notwithstanding the foregoing, to the extent that Children's agrees that it is not feasible to return or destroy such Protected Health Information, the terms and provisions of this Agreement shall survive termination of the Agreement and such Protected Health Information shall be used or disclosed solely for such purpose or purposes that prevented the return or destruction of such Protected Health Information.

7.0 INDEMNIFICATION.

Children's and Data Recipient shall each defend, indemnify and hold harmless the other from and against any and all claims, losses, causes of action, judgments, damages and expenses including, but

not limited to attorney's fees, to the extent caused by or arising out of any breach of this Agreement or failure to perform the obligations hereunder, by the indemnifying party, its employees, officers, volunteers or Contractors. The indemnity obligations set forth in this Section 6.0 shall survive termination of this Agreement.

8.0 **INJUNCTIVE RELIEF**.

Data Recipient agrees that the remedies at law for any breach by it of the terms of this Agreement shall be inadequate and that monetary damages from any such breach may not be sufficient or readily measured. Accordingly, in the event of any breach or threatened breach by Data Recipient of any terms of this Agreement, Children's shall be entitled to immediate injunctive relief. Children's right to injunctive relief shall be cumulative and nothing herein shall prohibit Children's from seeking all other available remedies.

9.0 **MISCELLANEOUS**.

9.1 Effect. The terms and provisions of this Agreement shall supercede any other conflicting or inconsistent agreements between Children's and Data Recipient, including without limitation all exhibits or other attachments hereto and all documents incorporated herein by reference. Without limiting the foregoing, any limitation of liability or exclusion of damages provisions in any other agreement shall not be applicable to this Agreement.

9.2 Amendment. Data Recipient and Children's agree to amend this Agreement to the extent necessary to allow either party to comply with the Privacy Rule, the Standards for Electronic Transactions (45 CFR Parts 160 and 162) and the Security Standards (45 CFR Part 142) (collectively, the "Standards") promulgated or to be promulgated by the Secretary or other regulations or statutes. Data Recipient agrees that it will fully comply with all such Standards and that it will agree to amend this Agreement to incorporate any material changes required by the Standards.

9.3 Correspondence. All notices or reports required by this Agreement will be sent to the following addresses or such other addresses as either party may designate in writing by first class mail, fax or hand delivery.

9.4 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Georgia, without regard for principles of choice of law.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives effective as of the day and year set forth above.

By: _____

Date: _____

ATTACHMENT A

List Protected Health Information included in Limited Data Set: