Policies and Procedures; Corporate

This policy is in effect for Children's Hospital of The King's Daughters Health System (CHKDHS) to include the following subsidiaries: Children's Hospital of The King's Daughters, Inc. (CHKD), Children's Medical Group, Inc., and CMG of North Carolina, Inc. (CMG), and Children's Surgical Specialty Group, Inc. (CSSG).

Individuals Reviewing: **Deborah L. Barnes**
VP/Information Services
Chief Information Officer

Sherri M. Matson, Esq.
VP/General Counsel

Jere Mundy, RHIA
Director, Health Information Mgmt.
Corporate Privacy Officer

Tina Allen
Director, Compliance and Internal Audit
Corporate Compliance Officer

Policy No.: C3416 **Effective Date**: March 2, 2016 **Previous Revision**: April 30, 2013

Dates Reviewed:

11/03	4/05	11/06	4/09	4/10	3/13	4/13	2/16

SUBJECT: HIPAA PRIVACY AND SECURITY RULE COMPLIANCE

POLICY: Compliance with the HIPAA Privacy Rule is part of the Corporate Compliance Program. Privacy Compliance is overseen by the Corporate Compliance Committee, its subcommittee, the Privacy and Security Subcommittee, and the Corporate Privacy Officer. All potential breaches in Children's Health System's (CHS) compliance with the HIPAA Privacy and Security Rule practices must be reported to the Corporate Privacy Officer.

PROCEDURE

A. Corporate Privacy Officer

1. Together with the Corporate Information Security Officer, the Corporate Compliance Officer, General Counsel, and the Privacy and Security Subcommittee are responsible for the development and implementation of the policies and procedures needed for compliance with the Privacy Rule and Security Rule by the health system.
2. Is responsible for receiving complaints about the health system's privacy practices and providing further information about matters covered by the notice.
3. Is responsible for coordinating the review of CHS privacy practices and, when necessary, the review of possible/potential breaches in privacy.
4. Is responsible for reporting HIPAA Privacy Rule compliance to the Corporate Compliance Committee at the Privacy and Security Subcommittee meetings and the management level Corporate Compliance Committee meetings.

B. Standard: Training.

1. CHS must train all members of its workforce on the policies and procedures with respect to protected health information required by the Privacy Rule and Security Rule as necessary and appropriate for the members of the workforce to carry out their function within the health system.

2. Implementation Specifications: Training.

   a. CHS must provide training that meets the requirements of paragraph B.1.of this policy, as follows:

      i. To each member of the CHS workforce (employees, students, volunteers, temporary staff – paid and unpaid) within a reasonable period of time after the person joins the workforce; and

      ii. To each member of the workforce whose functions are affected by a material change in the policies or procedures required by the Privacy Rule and Security Rule, within a reasonable period of time after the material change becomes effective.

   b. CHS must document that the training as described in paragraph B.2.a. of this section has been provided.

C. Standard: Safeguards.

1. CHS must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

2. Implementation specification: Safeguards.

   a. CHS must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Privacy Rule.

   b. CHS must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use of disclosure.

D. Standard: Complaints to CHS.

1. Individuals (patients/legal guardian) may make complaints concerning CHS policies and procedures required by the Privacy Rule or the Security Rule or its compliance with such policies and procedures or its or its Business Associates in compliance with the requirements of the Privacy Rule or Security Rule to the Corporate Privacy Officer. Individuals may be required to submit their complaints in writing. Complaints by individuals regarding the Privacy Rule and the Security Rule made to other CHS members must be forwarded to the Corporate Privacy Officer.

2. Implementation specification: documentation of complaints. All complaints received, and their disposition, if any, must be documented and forwarded to the Corporate Privacy Officer.

E. Standard: Sanctions.

1. CHS must apply appropriate sanctions against members of its workforce and professional staff who fail to comply with the privacy and security policies and procedures of CHS or the requirements of the Privacy Rule or the Security Rule. This standard does not apply to a member of the CHS workforce with respect to actions that are covered by and that meet the conditions of the Privacy Rule or the Security Rule pertaining to disclosures by whistleblowers and workforce member crime victims or paragraph G.2. of this section.

2. Implementation specification: documentation. CHS must document the sanctions that are applied, if any.

F. Standard: mitigation. CHS must mitigate, to the extent practicable, any harmful effect that is known to it concerning the use or disclosure of protected health information in violation of its policies and procedures or the requirements of the Privacy Rule or the Security Rule by CHS or its business associates.

G. Standard: refraining from intimidating or retaliatory acts. CHS may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by the Privacy Rule or the Security Rule, including the filing of a complaint;

2. Individuals and others. Any individual or other person for:

    a. Filing of a complaint with the Secretary under subpart C of part 160 of the Privacy Rule;

    b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

    c. Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the Privacy Rule.

H. Standard: Waiver of Rights. CHS may not require individuals to waive their rights under the Privacy Rule to complain to the HHS Secretary as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

I. Standard: policies and procedures.

1. CHS must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of the Privacy Rule and the Security Rule. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of the Privacy Rule or the Security Rule.

2. Standard: changes to policies or procedures.

    a. CHS must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of the Privacy Rule and the Security Rule;

    b. When CHS changes a privacy practice that is stated in its Notice of Privacy Practices, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision because it has included in its Notice a statement reserving its right to make such a change in its privacy practices; or

    c. CHS may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph I.5. of this section.

3. Implementation specification: changes in law. Whenever there is a change in law that necessitates a change to policies or procedures, CHS must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice of Privacy Practices, CHS must promptly make the appropriate revisions to the Notice and obtain a new written acknowledgement from the individual.

4. Implementation specifications: changes to privacy practices stated in the notice.

    a. To implement a change as provided by paragraph I.2.a. of this section, CHS must:

        i. Ensure that the policy or procedure, as revised to reflect a change in the privacy practice as stated in its Notice, complies with the standards, requirements, and implementation specifications of the Privacy Rule;

        ii. Document the policy or procedure, as revised, as required by paragraph J. of this section; and;

        iii. Revise the Notice to state the changed practice and make the revised Notice available to the individuals with written acknowledgement. CHS may not implement a change to a policy or procedure prior to the effective date of the revised notice.

5. Implementation specification: changes to other policies or procedures. CHS may change, at any time, a policy or procedure that does not materially affect the content of the Notice, provided that:
    a. The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of the Privacy Rule; and;
    b. Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph J. of this section.

J. Standard: documentation.

1. CHS must:
    a. Maintain the policies and procedures provided for in paragraph I of this section in written or electronic form;
    b. If a communication is required by the Privacy Rule to be in writing, maintain such writing, or an electronic copy, as documentation; and;
    c. If an action, activity, or designation is required by the Privacy Rule to be documented, maintain a written or electronic record of such action, activity, or designation.
2. Implementation specification: retention period. CHS must retain the documentation required by paragraph J.1. of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.