	Type of Policy: System-Wide **System-Wide policies apply to ALL workforce at CHKDHS as a whole.**
	POLICY TITLE: (#C3416) HIPAA Privacy & Security Rule Compliance
	Effective Date: (June 3, 2022) (Previous Version Date: May 13, 2019)

POLICY:

Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule is part of the Corporate Compliance Program. HIPAA Privacy compliance is overseen by the CHS Board Compliance Oversight Committee, the Corporate Compliance Committee (Committee), its subcommittee, the Privacy and Security Subcommittee (Subcommittee), and the CHKDHS Privacy Officer. All potential HIPAA Privacy breaches in CHKDHS' compliance with the HIPAA Privacy and Security Rule practices must be reported to the CHKDHS Privacy Officer.

PROCEDURE:

A. CHKDHS Privacy Officer

1. Together with the CHKDHS Corporate Information Security Officer, the CHKDHS Corporate Compliance Officer, the CHKDHS General Counsel, and the Subcommittee are responsible for the development and implementation of the policies and procedures needed for compliance with the HIPAA Privacy Rule and Security Rule by the Health System.
2. Is responsible for receiving complaints about the Health System's HIPAA Privacy practices and providing further information about matters covered by the Notice of Privacy Practices form (Notice).
3. Is responsible for coordinating the review of CHKDHS' HIPAA Privacy practices and, when necessary, the review of possible/potential breaches in HIPAA Privacy.
4. Is responsible for reporting HIPAA Privacy Rule compliance to the Committee and CHS Board Oversight Committee meetings.

B. Standard: Training.

1. CHKDHS must annually train all workforce members on the policies and procedures with respect to protected health information (PHI) required by the Privacy Rule and Security Rule as necessary and appropriate for the workforce members to carry out their function within the Health System.
2. Implementation Specifications: Training.
   a. CHKDHS must provide training that meets the requirements of paragraph B.1.of this policy, as follows:
      i. To each member of the CHKDHS workforce (employees, students, volunteers, temporary staff – paid and unpaid) within a reasonable period of time after the individual 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 HIPAA Privacy Rule and Security Rule, within a reasonable period of time after the material change becomes effective.
   b. CHKDHS must document that the training as described in paragraph B.2.a. of this section has been provided.

C. Standard: Safeguards.

1. CHKDHS must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.
2. Implementation Specification: Safeguards.
    a. CHKDHS must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the HIPAA Privacy Rule.
    b. CHKDHS must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use of disclosure.

D. Standard: Complaints to CHKDHS.
1. Individuals may make complaints concerning CHKDHS policies and procedures required by the HIPAA Privacy Rule or the Security Rule or its compliance with such policies and procedures or its business associates in compliance with the requirements of the HIPAA Privacy Rule or Security Rule to the CHKDHS Privacy Officer or their designee. Individuals may be required to submit their complaints in writing. Complaints by individuals regarding the HIPAA Privacy Rule and the Security Rule made to other CHKDHS workforce members must be forwarded to the CHKDHS Privacy Officer or their designee.
2. Implementation Specification: Documentation of Complaints. All complaints received, and their disposition, if any, must be documented by the CHKDHS Privacy Officer or their designee.

E. Standard: Sanctions.
1. CHKDHS must apply appropriate sanctions against members of its workforce (including professional staff) who fail to comply with the HIPAA Privacy and Security policies and procedures of CHKDHS or the requirements of the HIPAA Privacy Rule or the Security Rule. This standard does not apply to a member of the CHKDHS workforce with respect to actions that are covered by and that meet the conditions of the HIPAA Privacy Rule or the Security Rule pertaining to disclosures by whistleblowers and workforce member crime victims or paragraph G.2.below.
2. Implementation Specification: Documentation. CHKDHS must document the sanctions that are applied, if any. See System-Wide Policy #C6120, HIPAA Corrective Action.

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

G. Standard: Refraining from Intimidating or Retaliatory Acts. CHKDHS 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 HIPAA 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 of the U.S. Department of Health and Human Services (Secretary) under subpart C of part 160 of the HIPAA 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 PHI in violation of the HIPAA Privacy Rule.

H. Standard: Waiver of Rights. CHKDHS may not require individuals to waive their rights under the HIPAA Privacy Rule to complain to the 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. CHKDHS must implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA 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 PHI 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 HIPAA Privacy Rule or the Security Rule.
2. Standard: Changes to Policies or Procedures.
    a. CHKDHS 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 HIPAA Privacy Rule and the Security Rule;
    b. When CHKDHS changes a privacy practice that is stated in its Notice of Privacy Practices (Notice), and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI 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. CHKDHS 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, CHKDHS must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice, CHKDHS 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, CHKDHS 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 HIPAA Privacy Rule;
        ii. Document the policy or procedure, as revised, as required by paragraph J. below and;
        iii. Revise the Notice to state the changed practice and make the revised Notice available to the individuals with written acknowledgement. CHKDHS 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. CHKDHS 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 HIPAA 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.below.

J. Standard: Documentation.

1. CHKDHS must:
    a. Maintain the policies and procedures provided for in paragraph I above in written or electronic form;
    b. If a communication is required by the HIPAA 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 HIPAA Privacy Rule to be documented, maintain a written or electronic record of such action, activity, or designation.
2. Implementation Specification: Retention Period. CHKDHS must retain the documentation required by paragraph J.1. of this section for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

REFERENCE:

45 C.F.R. § 164.530
45 C.F.R. § 160.316
45 C.F.R. § 164.520

RELATED DOCUMENTS:

System-Wide Policy #C6120 HIPAA Corrective Action

INDIVIDUALS REVIEWING:
Kimberly S. Day, Esq., Vice President/General Counsel
Joseph Hooks, Chief Technology Officer
Laura Doty, Director, Health Information Management
Tina Allen, Director, Compliance & Internal Audit/Compliance & Privacy Officer

Policy Owner, John P. Harding, Sr. Vice President/COO

This policy is in effect for Children's Hospital of The King's Daughters Health System (CHKDHS) including but not limited to the following subsidiaries: Children's Hospital of The King's Daughters, Incorporated (CHKD), Children's Medical Group, Inc. , and CMG of North Carolina, Inc.(CMG), and Children's Surgical Specialty Group, Inc. (CSSG).