CHILD HEALTH AND DEVELOPMENT INSTITUTE OF CONNECTICUT, INC.

HIPAA SECURITY & PRIVACY POLICIES

TABLE OF CONTENTS

Page

KEY HIPAA DEFINITIONS……1

Overview of Requirements Relating to Required and Addressable Implementation Specifications in the Security Standards……...6

ADMINISTRATIVE SAFEGUARDS

Security Management - Risk Analysis and Mitigation Policy.....13

Security Management – Risk Management Policy.....15

Security Management – Sanction Policy……16

Security Management - Information System Activity Review Policy……18

Security Management Responsibility - Assignment of Security Responsibility Policy……...19

Workforce Security - Access Authorization and Supervision Policy……..20

Workforce Security – Workforce Clearance Policy……22

Workforce Security – Workforce Termination Policy……24

Information Access Management – Access Authorization Policy……..26

Information Access Management – Access Establishment and Modification Policy……...……27

Security Awareness and Training – Security Reminders Policy…….28

Security Awareness and Training - Malicious Software Policy……..30

Security Awareness and Training - Login Monitoring Policy……32

Security Awareness and Training - Password Management Policy……33

Security Incident Procedures - Response & Reporting Policy……37

Contingency Plan – Data Backup Policy…….40

Contingency Plan – Disaster Recover Policy……..41

Contingency Plan – Emergency Mode Operations Policy……..43

Contingency Plan – Testing and Revision Policy……...44

Contingency Plan - Application and Data Criticality Analysis Policy……...46

Evaluation – Compliance Evaluation Policy……...47

Business Associate Contracts and Other Arrangements – Use and Disclosure of Protected Health Information and Business Associate Agreement Requirements Policy……...49

PHYSICAL SAFEGUARDS

Facility Access Controls – Facility Contingency Operations Policy……..50

Facility Access Controls – Facility Security Policy……51

Facility Access Controls – Facility Access Control and Validation Policy……...53

Facility Access Controls – Facility Maintenance Records Policy……..55

Workstation Use – Workstation Use Policy……57

Workstation Use – Workstation Security Policy…….59

Device and Media Controls – Device Disposal Policy……61

Device and Media Controls – Media Re-Use/Transfer Policy……63

Device and Media Controls – Accountability Policy……..64

Device and Media Controls – Data Backup and Storage Policy…….65

TECHNICAL SAFEGUARDS

Access Control – Unique User Identification Policy……...66

Access Control – Emergency Access Policy……...67

Access Control – Automatic Logoff Policy……68

Access Control – Encryption & Decryption Policy…….69

Access Control – Audit Controls Policy……..70

Integrity – Mechanism to Authenticate ePHI Policy……...72

Person or Entity Authentication – Person/Entity Authentication Policy…….....73

Transmission Security – Transmission Integrity Controls Policy……...74

Transmission Security – Transmission Encryption Policy……..75

HIPAA Security Rule Recordkeeping Policy……..76

PRIVACY PROTECTIONS

Use and Disclosure of Protected Health Information Subject to the Minimum Necessary Requirement Policy……77

Accounting of Disclosures of Protected Health Information Policy……...79

Notification of Breach of Protected Health Information Policy……80

Privacy Protection Policy……90

Certain Additional Privacy Protections for Protected Health Information Policy……97

KEY HIPAA DEFINITIONS
For Reference Only

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in the Administrative Safeguards, Physical Safeguards, and Technical Safeguards Policies.)

Administrative safeguards are administrative actions, and policies and procedures that address how the selection, development, implementation, and maintenance of security measures that protect electronic protected health information are managed and how workforce conduct is managed in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Business Associate means a person or entity who, on behalf of a Covered Entity, and other than in the capacity of a workforce member: creates, receives, maintains or transmits protected health information for a function or activity regulated by HIPAA; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

CHDI or *Child Health and Development Institute* means the Child Health and Development Institute of Connecticut, Inc.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity is any person or entity that is (a) a health care provider that conducts certain transactions in electronic form; (b) a health care clearinghouse; or (b) a health plan; and for which the Child Health and Development Institute performs or assists in the performance of a function or activity that involves the use or disclosure of protected health information, or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside of the Covered Entity or the Child Health and Development Institute.

Electronic Media means:

(1) Electronic storage media on which data is or may be recorded electronically, including, without limitation, memory devices in computers (hard

drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet, intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic Protected Health Information ("ePHI") means Protected Health Information transmitted by or maintained in any Electronic Media.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Health Care Operations includes functions of a Covered Entity or of Child Health and Development Institute on behalf of a Covered Entity such as:

- quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that acquiring generalizable knowledge is not the primary purpose of any study resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; and accreditation, certification, licensing, or credentialing activities;
- conducting or arranging for medical review, legal services, and auditing functions, including health care fraud and abuse detection or compliance;
- business planning and development, including cost management and planning related analysis; and
- business management and general administrative activities, including HIPAA compliance; customer service; resolution of complaints; transfer upon sale, transfer, merger or consolidation of the Covered Entity; creating de-identified health information; and fundraising.

HIPAA or the *HIPAA Standards* means the Health Insurance Portability and Accountability Act of 1996 and implementing privacy regulations codified at 45 C.F.R. parts 160 and 164 and security regulations codified at 45 C.F.R. parts 160, 162 and 164, as amended from time to time.

Individual means the person who is the subject of the Protected Health Information.

Individually Identifiable Health Information means information, including demographic information, collected from an individual, provided the information:

- Is created or received by the Covered Entity or by the Child Health and Development Institute on behalf of the Covered Entity;
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- Identifies the individual or leaves a reasonable basis on which to believe the information could be used to identify the individual.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Marketing means to make a communication about a product or service, directly or by arrangement with another entity, to encourage recipients of the communication to purchase or use the product or service. *Marketing* does not include a communication made to an individual:

- To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the Covered Entity in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication.
- For treatment and health care operations purposes, except where the Covered Entity receives financial remuneration in exchange for making the communication, including: for treatment of an individual by a health care provider, such as case management or care coordination for that individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual; to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the

communication; or for case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Password means confidential authentication information composed of a string of characters.

Payment means activities undertaken by the Covered Entity or by the Child Health and Development Institute on the Covered Entity's behalf to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, certain collection activities, medical necessity determinations, and utilization review.

Personal Representative means a person who has legal authority to make decisions related to health care on behalf of another person.

Physical safeguards are physical measures, policies, and procedures that address how electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information ("PHI") means Individually Identifiable Health Information in any form relating to the past, present or future physical or mental health condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual. PHI does not include Individually Identifiable Health Information regarding a person who has been deceased for more than fifty (50) years.

Secretary means the Secretary of the Department of Health and Human Services ("DHHS") or any other person or organization to whom authority is delegated.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Officer means an individual designated by the Child Health and Development Institute who is responsible for the development and implementation of the Child Health and Development Institute's security policies and procedures required by HIPAA. *Security Officer*, as used in these policies, may also include or refer to certain other individuals designated by the Child Health and Development Institute to carry out certain obligations and functions related to the Child Health and Development Institute's HIPAA policies and procedures.

Subcontractor means a person to whom CHDI delegates a function, activity, or service, other than in the capacity of a member of CHDI's workforce.

Technical safeguards means the technology and the policy and procedures that address how Electronic Protected Health Information is protected and how access to it is controlled.

Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to the individual, or referral of an individual to another provider for health care.

Unsecured Protected Health Information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary.

Use means the sharing, employment, application, utilization, examination, or analysis of PHI by the Covered Entity or by the Child Health and Development Institute on behalf of the Covered Entity.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Overview of Requirements Relating to Required and Addressable Implementation Specifications in the Security Standards

The HIPAA Security Rule includes security standards (the "Security Standards") and implementation specifications ("Specifications"). Covered entities and business associates are required to comply with all of the Security Standards with respect to the ePHI that they create, receive, maintain, or transmit. The Specifications serve as instructions for implementing the Security Standards and are categorized as "required" or "addressable." The "required" Specifications must be implemented, as these Specifications are deemed essential to the effective protection of ePHI by covered entities and business associates. The addressable Specifications are not required to be implemented and are intended to give covered entities and business associates flexibility in complying with the Security Standards. However, to comply with the Security Standards that contain addressable Specifications, covered entities and business associates are required to:

(1) Assess whether each Specification is a reasonable and appropriate safeguard in their environment, when analyzed with reference to the likely contribution to protecting ePHI; and

(2) As applicable to the covered entity or business associate:
- (a) Implement the Specification if reasonable and appropriate; or
- (b) If implementing the Specification is not reasonable and appropriate:
  - (i) Document why it would not be reasonable and appropriate to implement the Specification; and
  - (ii) Implement an equivalent alternative measure if reasonable and appropriate.

In implementing the Security Standards, including the required and addressable Specifications, covered entities and business associates can use any security measures that allow such entity to reasonably and appropriately implement the respective Security Standards and Specifications. In deciding which security measures to use, covered entities and business associates need to take into account the following factors:

(1) Their size, complexity, and capabilities;
(2) Technical infrastructure, hardware, and software security capabilities;
(3) The costs of security measures; and
(4) The probability and criticality of potential risks to ePHI.

Furthermore, to continue providing reasonable and appropriate protection of ePHI, the Security Standards require covered entities and business associates to review and modify as needed the Specifications that they implement to comply with the Security Standards, and update documentation of such Security Standards as needed.

****

The policies herein that address the Security Standards (as opposed to the Privacy Standards) are noted at the top of the first page of each policy as either "required" or "addressable." There are certain Security Standards and Specifications that are so closely related that implementing a policy for each would create duplicative information. Therefore, in a few instances, one policy addresses both a Security Standard and its Specification(s).

Attached is a list of the Security Standards and Specifications for your reference. The Security Standards are marked with the word "Standard." The Specifications are indented under the relevant Security Standard and each is identified as either addressable or required.

Security Standards and Implementation Specifications

Administrative Safeguards

STANDARD: Security Management Process – Implement policies and procedures to prevent, detect, contain, and correct security violations.

> Risk Analysis (required) – Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the covered entity.
>
> Risk Management (required) – Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
>
> Sanction Policy (required) – Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures.
>
> Information System Activity Review (required) – Implement procedures to regularly review records of information system activity (i.e. audit logs, access reports and security incident tracking reports).

STANDARD: Security Responsibility – Identify the security official who is responsible for the development and implementation of the HIPAA security policies and procedures.

STANDARD: Workforce Security – Implement policies and procedures to ensure that all workforce members have appropriate access to ePHI and prevent those workforce members who do not have access to ePHI from obtaining access to ePHI.

> Authorization and/or Supervision (addressable) – Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.
>
> Workforce clearance procedure (addressable) – Implement procedures to determine that a workforce member's access to ePHI is appropriate.
>
> Termination procedure (addressable) – Implement procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member ends or as may be required.

STANDARD: Information Access Management – Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of HIPAA's Privacy Rule.

> Access Authorization (addressable) – Implement policies and procedures for granting access to ePHI through access to a workstation, transaction, program, process, or other mechanism.

Access Establishment and Modification (addressable) – Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

STANDARD: Security Awareness and Training - Implement a software awareness and training program for all workforce members.

Security reminders (addressable) – Provide periodic security updates.

Protection from malicious software (addressable) – Implement procedures for guarding against, detecting, and reporting malicious software.

Log-in monitoring (addressable) – Implement procedures for monitoring log-in attempts and reporting discrepancies.

Password management (addressable) – Implement procedures for creating, changing, and safeguarding passwords.

STANDARD: Security Incident Procedures – Implement policies and procedures to address security incidents.

Response and Reporting (required) – Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

STANDARD: Contingency Plan – Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI.

Data Backup Plan (required) – Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

Disaster Recovery Plan (required) – Establish (and implement as needed) procedures to restore any loss of data.

Emergency Mode Operation Plan (required) – Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

Testing and Revision Procedures (addressable) – Implement procedures for periodic testing and revision of contingency plans.

Applications and Data Criticality Analysis (addressable) – Assess the relative criticality of specific applications and data in support of other contingency plan components.

STANDARD: Evaluation – Periodically evaluate the effectiveness of the security policies and procedures in light of environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures satisfy the Security Standards and Specifications.

STANDARD: Business Associate Contracts and Other Arrangements – A covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

Written Contract or Other Arrangement (required) – Document the satisfactory assurances required by the "Business Associate Contracts and Other Arrangements" Standard through a written contract or other arrangement with the business associate that satisfies other HIPAA Security Rule requirements.

Physical Safeguards

STANDARD: Facility Access Controls – Implement policies and procedures to limit physical access to the electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Contingency Operations (addressable) – Establish procedures that provide authorized individuals in an emergency to access the facility to restore lost data when operating under a disaster recovery plan and emergency mode operations plan.

Facility Security Plan (addressable) – Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Access Control and Validation Procedures (addressable) – Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Maintenance Records (addressable) – Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (i.e. hardware, walls, doors and locks).

STANDARD: Workstation Use – Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be

performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

STANDARD: Workstation Security – Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.

STANDARD: Device and Media Controls – Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility.

> Disposal (required) – Implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored.
>
> Media Re-use (required) – Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
>
> Accountability (addressable) – Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
>
> Data Backup and Storage (addressable) – Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Technical Safeguards

STANDARD: Access Control – Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

> Unique User Identification (required) – Assign a unique name and/or number for identifying and tracking user identity.
>
> Emergency Access Procedure (required) – Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
>
> Automatic Logoff (addressable) – Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
>
> Encryption and Decryption (addressable) – Implement a mechanism to encrypt and decrypt ePHI.

STANDARD: Audit Controls – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

STANDARD: Integrity – Implement policies and procedures to protect ePHI from improper alteration or destruction.

Mechanism to Authenticate ePHI (addressable) – Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

STANDARD: Person or Entity Authentication – Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

STANDARD: Transmission security – Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Integrity Controls (addressable) – Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

Encryption (addressable) – Implement a mechanism to encrypt ePHI whenever deemed appropriate.

STANDARD: Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the Security Standards and Specifications.

STANDARD: Documentation Requirements – Implement reasonable and appropriate policies and procedures to comply with the Security Standards and Specifications in written form. Maintain a written record of any action, activity, or assessment that is required by a Security Standard or Specification.

Time Limit (required) – Retain the documentation required under the Security Rule for six (6) years from the later of the date the documentation was created or the date when it last was in effect.

Availability (required) – Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Updates (required) – Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Security Management – Risk Analysis and Mitigation Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies as part of its security management process with applicable laws regarding security risk analysis and mitigation.

POLICY:

It is the policy of CHDI to conduct periodic security risk assessments whereby potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI CHDI creates, receives, maintains or transmits are analyzed and mitigated (the "Risk Assessment"). The Risk Assessment will include the identification and documentation or hazards of: the information systems that store ePHI; the risks and vulnerabilities to those information systems; the threats or hazards that could act upon the risks and vulnerabilities; a ranking of security risks and vulnerabilities uncovered based on the severity of the risk and vulnerability, and a plan for mitigating those risks and vulnerabilities.

PROCEDURES:

1. The Security Officer is responsible for ensuring that a Risk Assessment is performed.

2. The Security Officer is responsible for ensuring that the Risk Assessment is reviewed and updated annually to keep security measures current.

3. When reviewing and updating the Risk Assessment, the Security Officer considers all relevant possible losses of ePHI, including losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur, and identifies and documents all information systems that store ePHI, the potential vulnerabilities associated with each information system (in terms of both frequency and magnitude of damage), and the potential threats or hazards that could act upon each information system.

4. The Security Officer is responsible for preparing a written plan for mitigation ("Mitigation Plan") to bring the risk level associated with each information system to a reasonable and appropriate level permitted by HIPAA.

5. The Mitigation Plan shall consider security measures already in place, possible security measures to be implemented, the cost of implementing such measures, the possibility of implementing such measures, and the probability and criticality of potential risks to ePHI.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Security Management – Risk Management Policy

PURPOSE:

The purpose of this policy is to comply with applicable laws regarding security risk management.

POLICY:

It is the policy of CHDI to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and acceptable level to comply with HIPAA. To carry out this policy, a formal documented plan for managing security risks and vulnerabilities to ePHI will be implemented. Such plan shall ensure the confidentiality, integrity and availability of all ePHI that is created, received, maintained or transmitted, protect against reasonably anticipated threats or hazards to security or integrity of such ePHI and protect against reasonably anticipated uses or disclosures of such ePHI. The plan will include the assignment of responsibilities and the implementation of a continuous monitoring, feedback, and assessment process.

PROCEDURES:

1. The Security Officer is responsible for all tasks related to risk management. Such risk management tasks shall include, but not be limited to:

    a) reducing identified risks to reasonable and appropriate levels.

    b) monitoring security risks to all information systems that hold ePHI throughout the year, including information systems security reviews and providing feedback to the appropriate workforce members.

    c) auditing and updating the Risk Assessment no less than once per year.

    d) in coordination with human resources, enforcing sanctions for violations of HIPAA security policies.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Security Management - Sanction Policy

PURPOSE:

The purpose of this policy is to ensure that all workforce members of Child Health and Development Institute comply with applicable laws regarding security of ePHI.

POLICY:

It is the policy of CHDI to appropriately discipline and sanction workforce members for any violation of the CHDI's HIPAA security policies and procedures, and that the discipline and sanctions will be fairly applied and commensurate with the gravity of the violation. This policy is implemented as an effective step to minimize risks and vulnerabilities to the ePHI of CHDI.

PROCEDURES:

1. The Security Officer will instruct all workforce members in proper handling of actual or reasonably suspected security violations and incidents.

2. All workforce members are responsible for reporting actual or reasonably suspected security violations and incidents to the Security Officer.

3. The Security Officer will receive and document all security violations and incidents, and investigate such violations and incidents in a timely manner.

4. CHDI will not retaliate against any individual who reports a violation of any HIPAA security policy or procedure or who reports a security violation or incident.

5. The Security Officer and his or her designee, working with human resources, will review policy and procedure violations or incident involving workforce members and recommend corrective or disciplinary measures. Such measures will be fairly applied and commensurate with the gravity of the violation. A workforce member's good faith efforts to comply with CHDI's security policies and procedures or to mitigate risk or harm of a security violation or incident may be taken into account when imposing sanctions.

6. Failure to comply with CHDI's security policies and procedures will result in disciplinary action, up to and including termination, in accordance with

this Sanction Policy and CHDI's human resources Discipline policy, or in the case of outside affiliates, termination of the affiliation.

7. Corrective or disciplinary measures will include, but not be limited to:

   a) Re-training;

   b) Removal of access or other authorizations;

   c) Verbal and written warnings;

   d) Termination.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Security Management - Information System Activity Review Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding reviewing information systems activity.

POLICY:

It is the policy of CHDI to monitor and review systems that store, access, and transmit ePHI. The level of monitoring and reviewing will be commensurate with the level of risk inherent in the system as set forth on the CHDI's Risk Assessment.

PROCEDURES:

1. The Security Officer is responsible for ensuring that information systems activity is monitored and reviewed at intervals commensurate with their associated risk level, but not less than once per year. Such information systems activity includes security incidents, information system audit logs, activity reports, access reports, logins, file access or other mechanisms that document information system activity. The Security Officer may designate one or more individuals to assist in monitoring and reviewing and will provide such individuals with a listing of workforce authorizations.

2. Information system activity records, including, but not limited to, information system-generated activity reports and manually-prepared log files, incident reports, and other documentation are maintained and archived for no less than seven (7) years.

3. The Security Officer is responsible for ensuring that a formal audit of the information system activity monitoring and review process is performed periodically, but not less than once per year.

4. Any exceptions and unauthorized access attempts noted by any workforce member or in the information systems monitoring and review process must be reported to the Security Officer immediately for response.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Security Management –Assignment of Security Responsibility Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding assignment of ePHI security responsibility.

POLICY:

It is the policy of Child Health and Development Institute to assign the responsibility for security of ePHI to one qualified individual.

PROCEDURES:

Assignment of Security Responsibility

1. CHDI has appointed one qualified individual to have final responsibility for CHDI's security of ePHI. This individual will be referred to as the Security Officer. The Security Officer may delegate certain security tasks to workforce members of CHDI or to outside vendors as long as the Security Officer maintains proper oversight and remains responsible for security of ePHI.

2. The Security Officer is responsible for the development and implementation of the CHDI's policies and procedures regarding security of ePHI.

3. The Security Officer is authorized to utilize legal counsel as necessary to comply with the HIPAA Security Rule.

4. All workforce members, affiliates, vendors and other third parties are informed of the name of the Security Officer.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Workforce Security - Access Authorization and Supervision Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding authorization to and supervision of ePHI.

POLICY:

It is the policy of CHDI to categorize levels of access to ePHI that are necessary at CHDI for each position (based upon the minimum access necessary to perform the duties of the position), to properly supervise workforce members' access to ePHI.

PROCEDURES:

Access Authorization, Modification and Establishment

1. The Security Officer grants workforce members reasonable and appropriate levels of access to ePHI that are necessary at CHDI based upon such workforce member's position and job description.

2. The Security Officer is responsible for granting, establishing and modifying access rights or privileges to systems, applications, programs, devices or equipment, and all means of access (remote, wireless, etc.) using the available electronic (technical) features and functionality of each system.

3. The Security Officer is responsible for determining and documenting the appropriate category of access to ePHI for workforce members who require access to ePHI to perform their job functions, and for personnel who perform their job functions in areas where ePHI is located, but who do not need ePHI to perform their job functions, including maintenance workers and front desk and reception staff, on an Access Authorization list attached hereto.

4. Once the level of access to ePHI is determined for a workforce member, the Security Officer is responsible for electronically granting the appropriate access and/or privileges for each information system and communicating this to Human Resources for inclusion in job descriptions

and to the individual responsible for granting appropriate access, rights, and privileges to the information systems, applications and equipment.

Supervision

1. The Security Officer is responsible for determining and documenting reasonable and appropriate levels of supervision that workforce members require to access ePHI.

2. The Security Officer and the Human Resources Official are responsible for ensuring that all workforce members, including maintenance workers, have proper supervision as they access ePHI.

General

1. The Security Officer shall upon a change in a workforce member's position or responsibilities review and modify, if necessary, such member's access authorization and supervision status.

2. The Security Officer will periodically, but not less than annually, perform an access authorization and supervision audit using randomly-selected workforce members accounts, observing the actual access to ePHI that workforce members have and the level of supervision administered during that access to ensure it complies with access granted or supervision required.

3. The Security Officer is responsible for determining the validity of and granting or denying all requests for changes in access authorization and supervision.

4. The Security Officer may grant workforce members a password in an emergency in compliance with this Access Authorization and Supervision Policy.

5. The Security Officer may grant access to information systems on a temporary basis by assigning a guest password to appropriate workforce members (vendors, service providers, temporary workforce members) and will revoke such password as soon as it is no longer required.

Authorization

1. Authorization for access to ePHI for outside contractors shall be described and set forth in any agreement between the outside contractor and CHDI.

2. The Security Officer is responsible for ensuring that contractors do not have access beyond that which is necessary for contract performance.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Workforce Security – Workforce Clearance Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding clearance of workforce members to access ePHI.

POLICY:

It is the policy of CHDI to conduct appropriate clearance procedures on all candidates for workforce positions that have access to ePHI commensurate with the level of risk to the information systems the workforce member will access.

PROCEDURES:

1. The Security Officer and appropriate human resources official are responsible for performing clearance procedures on all current workforce members and workforce candidates and documenting the results of those procedures. Workforce clearance is reassessed by the Security Officer periodically, but not less than annually.

    a) The level of clearance procedures of workforce members are commensurate with the level of risk to the information systems the workforce member will access, as determined by the position the workforce member holds or is a candidate for holding.

    b) The Security Officer is responsible for determining and documenting whether appropriate clearance procedures have been performed and whether the individual is cleared to access ePHI and authorizing such access in accordance with the Access Authorization Policy (see attached sample form). In the event that an individual is not cleared for access to ePHI, the Security Officer is responsible for promptly notifying human resources.

2. The Security Officer and the appropriate human resources official are responsible for determining and documenting the extent of clearance procedures necessary for each position based on the Risk Assessment. Clearance procedures may include, but are not limited to:

    a) Character References

    b) Academic Degrees

c) Professional Licenses

d) Past Employment Responsibilities

e) Credit Check

f) Criminal Background Check

3. Human Resources is responsible for communicating changes in a workforce member's position to the Security Officer who then decides whether additional clearance procedures are required based upon the requirements of the new position.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Workforce Security – Workforce Termination Policy

PURPOSE:

The purpose of this policy is to ensure that CHDI complies with applicable laws regarding termination of workforce access to ePHI.

POLICY:

It is the policy of CHDI to prevent access to ePHI by workforce members who are no longer authorized to access such ePHI.

PROCEDURES:

1. Terminations and changes in workforce member positions or status will be promptly communicated by the human resources official to the Security Officer.

2. Upon termination of an arrangement with or employment of a workforce member, termination of an arrangement with an external contractor, or if a workforce member loses clearance to access ePHI in accordance with the Workforce Clearance Policy, the Security Officer is authorized to disable and/or remove access to information systems including, without limitation:

    a) Deactivating workforce member accounts,

    b) Resetting passwords, and

    c) Re-routing email accounts to the Security Officer's email account.

    The Security Officer determines when it is appropriate to perform the above procedures.

3. The Security Officer is responsible for periodically updating the Access Authorization List to document the change in access authorization and will provide the new list to those who require it.

4. The Security Officer or human resources official are responsible for retrieving the following, as appropriate:

    a) Physical media, devices, or equipment containing ePHI, and

b) Physical access control items (i.e. identification badges, swipe cards, tokens, keys, etc.).

The Security Officer determines when it is appropriate to perform the above procedures.

5. The Security Officer is responsible for determining whether physical access devices, such as locks, combinations for locks, etc., for areas where the affected workforce member was previously authorized, require changing, and if so, is authorized to have such changes made.

The contents of the affected workforce member's user directories, email archives and other information system data will be made available to the Security Officer, as appropriate, to determine or mitigate risk associated with the workforce member's use or disclosure of ePHI.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Information Access Management – Access Authorization Policy

PURPOSE:

The purpose of this policy is to ensure that CHDI complies with applicable laws regarding access to ePHI.

POLICY:

It is the policy of CHDI to implement security measures to grant access to ePHI, ensure that personnel needing access to ePHI have appropriate access, and restrict persons who do not require access to ePHI from obtaining such access.

PROCEDURES:

1. Access to ePHI will only be granted through a secured system. This system may be a workstation for which an ID and password is needed to access ePHI, a program for which an ID and password is required, a transaction which must be encrypted or otherwise protected, or a process or other mechanism that requires authorization.

2. The Security Officer is responsible for documenting all access authorizations and any changes in authorization for each workforce member to whom access is granted. The Security Officer shall grant only the access that is appropriate for the job in accordance with the Access Authorization and Supervision Policy and the Workforce Clearance Policy. The Security Officer will not grant access to a secured system until a properly-authorized request has been submitted and approved by the Security Officer.

3. No employee, manager or supervisor, other than the Security Officer, may authorize access for himself or herself. The Security Officer may authorize access for himself or herself, however CHDI's governing body shall periodically review such access.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Information Access Management – Access Establishment and Modification Policy

PURPOSE:

The purpose of this policy is to ensure that CHDI complies with applicable laws regarding access to ePHI.

POLICY:

It is the policy of CHDI to implement security measures to establish, document and review access to ePHI, ensure that personnel needing access to ePHI have appropriate access, and restrict persons who do not require access to ePHI from obtaining such access.

PROCEDURES:

1. The Security Officer is responsible for maintaining a master list of personnel and their respective access rights to workstations, transactions, programs and processes, and for updating such list in the event of any change to the access rights of one or more individuals. Examples of a change in access rights include an individual's termination or change in job role or function. The list will be maintained and reviewed in accordance with the Access Authorization and Supervision Policy, Workforce Clearance Policy, Workforce Termination Policy and Password Management Policy.

2. The Security Officer shall regularly review the master list to ensure that access rights for each individual are consistent with established policies and job roles and functions.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Security Awareness and Training – Security Reminders Policy

PURPOSE:

The purpose of this policy is to ensure that CHDI complies with applicable laws regarding security training and reminders.

POLICY:

It is the policy of CHDI to ensure that workforce members are aware of and trained on security of ePHI on a periodic basis in order to heighten awareness of security issues and anomalies and to help prevent security incidents. Such awareness and training will be provided to workforce members as reasonable and appropriate to carry out their job functions.

PROCEDURES:

Reminders

1. The Security Officer is responsible for periodically informing workforce members of their security responsibilities.

2. The Security Officer is responsible for reminding all workforce members, including management, in various ways and at various times about security of ePHI.

    a) Reminders will be given at least annually.

    b) Reminders may include, but not be limited to:

        i) A notice on a workforce member's paycheck or direct deposit advice.

        ii) Posters.

        iii) A notice on a computer monitor or terminal upon logging in.

        iv) Pamphlets or memos from the Security Officer and department managers or supervisors.

3. The Security Officer is responsible for designing security reminders so that they supplement and reinforce training.

4. The Security Officer is responsible for ensuring that current security issues and/or incidents are communicated to workforce members on a timely basis based upon the risk level to the organization.

5. The Security Officer is responsible for ensuring that changes in security policy and procedures are communicated to workforce members on a timely basis.

Training

1. The Security Officer is responsible for determining when and where training sessions on security of ePHI will be held and how many times a year they will be held, but not less than once annually.

2. The Security Officer is responsible for designing a training program whereby all workforce members, including management, upon hiring and periodically thereafter, are trained on the security policies and procedures and use of applicable information systems. The security training program may be part of other training programs. The training program is revised by the Security Officer as necessary to respond to environmental and operational changes affecting security of ePHI.

3. Upon completion of training, all users of information systems are required to pass an exam on the functionality of such systems prior to receiving their respective system logins.

4. Workforce members who are granted access to the system and who make frequent errors when using the system are required to be retrained in the appropriate areas of the respective system(s). In the event that such users continue to make errors after being retrained, such users will be subject to further action including, without limitation, losing their rights to access such system(s).

Business Associates and Outside Vendors

1. The Security Officer is responsible for ensuring that all agents, subcontractors and outside vendors are aware of and required to comply with the security policies and procedures, whether through contract language or otherwise, provided, however, agents, subcontractors and outside vendors who are not workforce members are not required to attend security training or receive security reminders.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Security Awareness and Training - Malicious Software Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding protecting ePHI from malicious software.

POLICY:

It is the policy of CHDI to protect its systems from the destructive or altering effects of malicious software and code (e.g. viruses, worms, etc.), to implement procedures to detect and remove such software and code, and to report malicious software and code.

PROCEDURES:

1. The Security Officer is responsible for periodically reviewing all information systems and program purchases for known security issues. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will periodically verify with such vendor that appropriate anti-virus software is being used on all systems.

2. The Security Officer will ensure that workforce members are not authorized to disable virus-checking in systems.

3. Workforce members will obtain express permission from the Security Officer in order to install or load non-approved software or other code onto CHDI computer resources. Workforce members receive training and reminders about malicious code and security incidents as per the Awareness and Training Policy. Workforce training includes, but is not limited to, proper downloading procedures and proper scanning of media and devices on an ad-hoc basis.

4. Personally-owned computer resources, such as a home-based PC, used by workforce members to connect to computer resources remotely, must be protected from malicious software and code.

5. All malicious code incidents must be reported to and logged by the Security Officer.

6. The Security Officer is responsible for analyzing all malicious code incidents to identify additional vulnerabilities to the information systems and considers implementation of protections against such future incidents as part of the Risk Assessment. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will periodically verify with the vendor that such analysis has been conducted and consideration has been given to additional protections against future incidents.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Security Awareness and Training - Login Monitoring Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding security of ePHI through login monitoring.

POLICY:

It is the policy of CHDI to monitor log-in attempts in order to detect and report login discrepancies such as unauthorized and/or failed log-in attempts and dual log-in attempts.

PROCEDURES:

1. The Security Officer is responsible for monitoring and reviewing login activity. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will periodically verify with such vendor that it is monitoring and reviewing login activity and that information systems are configured with login monitoring and reporting functionality.

2. Workforce members will alert the Security Officer of any login attempts deemed reasonably "suspect" by the workforce members within a reasonable period of time. The Security Officer shall require CHDI's information systems vendor to alert the Security Officer of any login attempts deemed reasonably "suspect" by the vendor within a reasonable period of time.

3. CHDI will determine and set a reasonable time of inactivity that will terminate a workforce member's workstation by automatic logoff.

4. Workforce members will receive training and reminders about login monitoring and reporting of discrepancies.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Security Awareness and Training - Password Management Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding creation, structure, use and management, changing and safeguarding of passwords.

POLICY:

It is the policy of CHDI to implement procedures to properly manage the creation, structure, use, management and safeguarding of passwords used by workforce members to access any network, system, device, program, equipment, or application that is used to access, create, transmit, receive or store ePHI.

PROCEDURES:

General Password Management:

1. All workforce members that access networks, systems, devices, programs, equipment, or applications used to access, create, transmit, receive, or store ePHI must be supplied with a unique user identification to access ePHI. Workforce Members shall not share assigned unique system identifiers (or login names) with any other person, unless for authorized IT support purposes.

2. All workforce members must supply a password in conjunction with their unique user identification to gain access to any network, system, device, program, equipment or application used to access, create, transmit, receive, or store ePHI.

3. All workforce members must create, structure and use their passwords as described in this Policy.

4. The password aging schedule and password structure rules will be set by CHDI based upon the risk-level of the network system, application, program, device, and equipment.

5. All workforce members must change their passwords on a schedule set by the Security Officer.

6. Whenever possible, network systems, applications, programs, devices, and equipment must be set to automatically require workforce members to create structure-compliant passwords and to change passwords on a preset schedule in accordance with this Policy.

7. All workforce members will receive training regarding the creation and use of passwords. Training will include but not be limited to, actions that will cause a password to be revoked.

8. The proper creation and use of passwords, including any changes in this Password Management Policy, will be covered periodically throughout the year as a reminder to workforce members.

9. The Security Officer is responsible for auditing workforce members' passwords on a random basis to ensure compliance with this policy.

10. Terminations and changes in position will be communicated to CHDI's Human Resources Official and Security Officer or Designee immediately to enable the Security Officer to revoke or modify a workforce members' password, if necessary, in accordance with the Access Authorization Policy. The revocation of workforce members' passwords will be performed upon workforce termination in accordance with the Access Authorization Policy.

11. Anonymous access, including the use of guest and public accounts, to any CHDI electronic resource is prohibited.

12. The Security Officer will revoke a workforce members' password if he/she has reasonable cause to believe the password has been created, used or disclosed in a manner not compliant with this Policy.

13. Wherever possible, CHDI's network systems, applications, programs, devices, and equipment must be configured to automatically disable a workforce members' password after six unsuccessful login attempts. Deactivation will last for a time period set and documented by the Security Officer based on the risk-level of the network systems, application, program, device, or equipment, but will not be less than twenty (20) minutes.

Password Creation and Structure:

1. Each workforce member shall create passwords that can be easily remembered.

2. The use of a "strong password" is required on all systems that will accommodate one. Strong passwords have the following characteristics: Passwords must be at least eight characters long and include at least one

number or symbol, one upper case letter, and one lowercase letter; they must not contain the user's name, user ID, or CHDI's name; and they must be different from previous categories. Passwords shall be encrypted for storage and transmission whenever available, or whenever deemed necessary by the risk analysis or evaluation.

3. System administrator or system supervisor passwords must be changed every 90 days.

4. Password controls shall force periodic password changes at least every ninety days whenever available. The Security Officer shall work with CHDI's information systems vendor to establish the appropriate period for periodic password changes.

5. Password controls shall lockout login accounts after six unsuccessful login attempts, whenever available.

6. Automatic log off or password protected screen savers shall be used on all systems when available. Electronic sessions will be automatically terminated after period of time deemed appropriate.

III. Password Use:

Workforce members will comply with the following rules regarding use of passwords:

1. All passwords must be changed according to the schedule set forth by CHDI.

2. Passwords must be different from previous passwords used for at least 5 cycles, and changed at least once every 90 days. Passwords shall not be shared with any other person.

3. Workforce members must not use the same password for gaining access to publicly available websites as they do for gaining access to CHDI's systems or applications.

4. Passwords must not be inserted into email messages or other forms of electronic communication.

5. Default administration-level passwords that come with systems, applications, or devices must be changed immediately.

6. Do not write passwords down and store them anywhere in your office or online. Do not store passwords in a file on ANY computer system or device (including PDA devices or lab equipment) without encryption. Do not reveal passwords to anyone, including family members, co-workers,

and supervisors, except when authorized or requested by the Security Officer.

7. If you feel that an account or password has been compromised, report the incident to the Security Officer immediately and change all passwords.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Security Incident Procedures – Response & Reporting Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding security incident response and reporting.

POLICY:

It is the policy of CHDI to implement procedures to enable CHDI to identify the suspected or known occurrence of a security incident, to enable workforce members or IT Systems to report the incident to the Security Officer, to mitigate the harmful effect of an incident known to CHDI to the extent practicable and to document the security incident and its outcome. For purposes of this policy, security incidents include breach of unsecured protected health information, whether such protected health information is in electronic or paper format, as defined in the Notification of Breach of Protected Health Information Policy.

PROCEDURES:

1. The Security Officer is responsible for responding to all security incidents, which shall include all attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with IT System operations.

2. The Security Officers is responsible for testing all responses to security incidents at least annually, or more often as deemed appropriate by the Risk Assessment. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to test responses to security incidents within the IT systems but will remain responsible for testing CHDI's responses (altering key management, etc.).

3. Workforce members should immediately report any actual or suspected security incidents to the Security Officer.

4. The Security Officer will periodically train workforce members on the procedures to take if they suspect or know of a security incident.

5. The Security Officer is responsible for ensuring that sufficient products and/or services are dedicated to the monitoring and reporting of security

incidents, including network activity and review of information system-generated incident reports, consistent with the Risk Assessment. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to ensure the adequacy of such products and services.

6. During a security incident, the Security Officer will take steps to mitigate the harmful effects of a security incident known to CHDI to the extent practicable (e.g. repairing damage, restoring IT Service).

7. The Security Officer will ensure that the following procedures are followed for a suspected or actual security incident:

   a. The Security Officer will document each security incident, including, but not limited to, the details of the incident, the response, the outcome, steps taken to mitigate harm and any changes to CHDI's risk assessment or security procedures to avoid reoccurrence of security incident.

   b. If the incident has or may inflict damage to information systems, it will be considered a critical incident.

      In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to ensure an appropriate response to any critical incident. An example of an appropriate response is that if a critical incident has occurred or is occurring, the affected information systems will be disconnected from the network immediately.

      The Security Office will work with CHDI's vendor to determine the method of compromise and the Security Officer will document such method(s) for all critical incidents.

      If an operating system has been compromised, the Security Officer will work with CHDI's vendor to take appropriate action, such as a complete reload of the operating system and the performance of all updates and patches.

   c. The Security Officer will re-check system activity logs and login reports for any suspicious activity and continue to monitor the system for a period of time deemed appropriate by the Risk Assessment.

   d. The Security Officer will change administrator passwords for operating systems and critical applications that contain ePHI after an actual security incident.

8. If the security incident involved a breach of protected health information or unsecured protected health information, the Security Officer will make any required notifications of breach, in accordance with the Notification of Breach of Protected Health Information Policy.

9. The Security Officer may report security incident to law enforcement personnel or other outside entities, if appropriate.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Contingency Plan – Data Backup Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding contingency planning and data backup.

POLICY:

It is the policy of CHDI to backup ePHI so that it is available in an emergency or other occurrence and can be restored in a timely basis.

PROCEDURES:

1. All ePHI is backed-up on tapes on a daily basis.

2. Media used for backing up ePHI is stored in a secure readily available location with controlled access as documented on the Risk Assessment. All outside vendors that share backup media are required to sign a Business Associate Agreement.

3. The Security Officer is responsible for ensuring that a log of backups and the physical movement and location of such backup media is maintained.

4. As soon as practicable, the Security Officer will retrieve and load backup media when necessary in an emergency or other occurrence. The order of the backup is in accordance with the Risk Assessment.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Contingency Plan – Disaster Recovery Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding contingency planning and disaster recovery.

POLICY:

It is the policy of CHDI to implement procedures that ensure the recovery of ePHI and all information systems that create, access, store, or transmit ePHI.

PROCEDURES:

1. The Security Officer is responsible for ensuring that any loss of ePHI and the information systems that create, access, store or transmit the ePHI are restored and recovered. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to ensure that the vendor has an appropriate disaster recovery plan.

2. A Disaster Recovery Plan has been established and includes, but is not limited to:

    a) All backup documentation including identification of critical data, information systems, programs, and support items, as well as the location of backup media, and the backup log.

    b) The location of all installation media and upgrade media, to support the reinstallation of all programs and applications at their current release or version level.

    c) A current schematic of the information systems' environment, infrastructure, and connectivity.

    d) A listing of workforce members, consultants, or third party vendors that are authorized to perform data recovery.

    e) Documentation to restore ePHI from backup media.

i) Documentation includes procedures to restore one information system or program as well as all information systems or programs in a total disaster scenario.

ii) Documentation resides in at least one off-site secure location and such location is documented such that all individuals authorized to perform data recovery may access it.

f) An information system criticality ranking listing of the order in which to restore the information.

g) A current disaster recovery key contact listing that includes contact information for the following:

i) Information system consultants, programmers, and service providers.

ii) Hardware and other equipment/device vendors.

iii) Program and application vendors.

iv) Telephone systems vendors.

3. The Security Officer is responsible for ensuring that the workforce members involved have the proper training and experience required to perform recovery functions.

4. The Security Officer is responsible for testing the Disaster Recovery Plan on an annual basis, or more often as deemed appropriate by the Risk Assessment.

5. The Security Officer or a committee established by the Security Officer evaluates the Disaster Recovery Plan and makes any appropriate changes at least annually.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Contingency Plan – Emergency Mode Operations Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding contingency planning and emergency mode operations.

POLICY:

It is the policy of CHDI to implement procedures to ensure the continuity of business processes during an emergency or disaster, and to ensure security of ePHI while operating in emergency mode.

PROCEDURES:

1. The Disaster Recovery Plan includes tasks and processes that enable the continuation of operations during an emergency or disaster. The Security Officer is responsible for ensuring these tasks are performed in an emergency or disaster.

2. Appropriate workforce members are trained on emergency operations upon hire and retrained on such operations on an as needed basis as determined by the Security Officer.

3. In the event of an emergency or disaster, the Security Officer is responsible for implementing appropriate security measures to protect the records manually prepared while in emergency mode. The measures will include, but are not limited to, the following:

    a) Physical access control to manual records,

    b) Secure storage of manual records,

    c) Controlled creation of manual records, and

    d) Appropriate conversion of manual records to ePHI after manual operations has ended.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Contingency Plan – Testing and Revision Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding contingency plan testing and revision.

POLICY:

It is the policy of CHDI to test the adequacy of the contingency plan policies on a periodic basis and to make appropriate revisions to such policies based upon the results of and knowledge gained during the testing process.

PROCEDURES:

1. The Security Officer is responsible for conducting a test of the contingency plan policies at least annually, by performing one or more of the following or other appropriate tests:

    a) Department-specific simulated (what-if) information system, network, program, or vendor failures.

    b) Real-time, short-term, shutdowns of selected information systems, networks, programs, devices, equipment and databases based on the risk of failure or the priority set forth in the Risk Assessment.

    c) Remove access to the physical location of the information systems.

    In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to perform appropriate testing.

2. The Security Officer is responsible for evaluating and documenting the ability to:

    a) Restore the information system.

    b) Use alternate information systems, networks, programs, devices, equipment and databases.

    c) Notify workforce members of an emergency or disaster.

The Security Officer is responsible for documenting the tests performed and the results of such tests and revising the contingency plan policy as necessary.

Child Health and Development Institute

Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Contingency Plan – Application and Data Criticality Analysis Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding contingency planning and application and data criticality analysis.

POLICY:

It is the policy of CHDI to implement procedures that rank the relative criticality of its systems on an annual basis, or more frequently in response to changes in CHDI's systems environment and Risk Assessment.

PROCEDURES:

1. The Security Officer will seek input from workforce members, as determined appropriate by the Security Officer, to ensure that sufficient information about CHDI's systems is gathered to support the criticality ranking of CHDI's systems.

2. The Security Officer will review the above information and prepare a ranked listing of systems based on criticality for review and comment by certain workforce members, as determined appropriate by the Security Officer.

3. The criticality listing will be reviewed by the Security Officer no less than annually, and this review will include comment period from workforce members, as determined by the Security Officer.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Evaluation - Compliance Evaluation Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws regarding compliance evaluation.

POLICY:

CHDI will review its Security Policies and Procedures for technical and non-technical viability, effectiveness, and compliance with the HIPAA Security Regulation on an annual basis or more frequently as determined by the Security Officer.

PROCEDURES:

1. The Security Officer will review CHDI's Policies and Procedures at least annually or upon the happening of one or more of the following events:

    a. Changes in the HIPAA Security or Privacy Regulations;

    b. New Federal, State, or local laws and regulations affecting security of ePHI;

    c. Changes in the Risk Assessment recommendations;

    d. Changes in the risk management process;

    e. Changes in CHDI's IT environment;

    f. Changes in CHDI's business processes with respect to IT; or

    g. A security incident.

2. The Security Officer will obtain feedback, comments, and other input regarding the policies and procedures from appropriate workforce members.

3. The Security Officer will interview the following individuals in order to obtain feedback:

a. The Human Resources Official;

b. Vendors that host or provide IT-related services to CHDI; and

c. Other individuals as specified by the Security Officer.

4. The Security Officer will consider the following when reviewing CHDI's policies and procedures:

   a. The number of security incidents that have occurred at CHDI,

   b. The number of workforce sanctions applied,

   c. The number of security incidents that have occurred at Business Associates, and

   d. The results of the annual Security Audit.

5. The Security Officer is responsible for implementing changes to security policies and procedures. The following steps are followed as part of this process:

   a. All recommended changes are communicated to the governing body for final approval.

   b. Upon approval, all changes are communicated to workforce members.

Child Health and Development Institute
Effective Date: July 1, 2014

— REQUIRED —

SUBJECT: Business Associate Contracts and Other Arrangements – Use and Disclosure of Protected Health Information and Business Associate Agreement Requirements Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable rules regarding when a business associate may use, disclose or receive protected health information from a covered entity.

POLICY:

It is the policy of CHDI to appropriately safeguard all protected health information created, received, maintained or transmitted on a covered entity's behalf.

PROCEDURES:

1. **Documentation of Satisfactory Assurances.** In accordance with HIPAA requirements, CHDI and each covered entity documents the satisfactory assurances that CHDI will appropriately implement to safeguard the protected health information through a written agreement ("Business Associate Agreement" or "Data Use Agreement") between the covered entity and CHDI.

2. **Privacy Protections in Business Associate Agreement.** The privacy protections specified in the Certain Additional Privacy Protections for Protected Health Information Policy are incorporated into Business Associate Agreements with covered entities.

3. **Compliance with Business Associate Agreement.** If CHDI knows of a pattern of activity or practice of the covered entity that constitutes a material breach or violation of the covered entity's obligation under the applicable Business Associate Agreement, the covered entity is promptly notified. If the covered entity's steps to cure the breach are unsuccessful, CHDI shall terminate the Business Associate Agreement or arrangement, if feasible.

4. **Downstream Business Associates.** If CHDI engages a subcontractor to create, receive, maintain, or transmit protected health information on its behalf, CHDI will document through a downstream Business Associate Agreement the satisfactory assurances of the subcontractor that it will appropriately safeguard such protected health information.

Child Health and Development Institute

Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Facility Access Controls – Facility Contingency Operations Policy

PURPOSE:

The purpose of this policy is to support disaster recovery operations and emergency mode operations by establishing procedures that allow access to the facility in the event of an emergency.

POLICY:

It is the policy of CHDI to establish and implement procedures that will allow access to the facility in the event of an emergency in order to support the data restoration efforts in furtherance of the Disaster Recovery Plan and the Emergency Operations Plan.

PROCEDURES:

1. The Security Officer has documented the actions that must be taken to gain access to the ePHI that resides in the facility under each emergency scenario – and this documentation is located in the Disaster Recovery Plan.

2. The Security Officer is responsible for working with the facilities coordinator or similar member of the workforce when responding to an emergency situation that involves the physical facilities.

3. When remote access to ePHI is not sufficient to restore ePHI to an acceptable level, every effort will be made to gain access to the physical facility by contacting individuals or entities listed on the Facility Contingency List. Such list includes: vendors, service providers, engineers, technicians, town officials, utilities, and consultants who can assist with issues relating to the physical facilities. The list will reside with the Disaster Recovery Plan.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Facility Access Controls – Facility Security Policy

PURPOSE:

The purpose of this policy is to safeguard the physical facilities and the assets therein, including information systems, programs, equipment, devices, etc. that store ePHI, from compromise, tampering, and theft, by preventing unauthorized access to the facilities.

POLICY:

It is the policy of CHDI to establish and implement procedures that will prevent unauthorized access to the physical facilities and the assets therein, including programs, equipment, devices, etc. that store ePHI.

PROCEDURES:

1. The various threats to the physical facilities and the assets therein have been documented and are maintained by the Security Officer.

2. The Security Officer will continually work with the workforce member who is responsible for physical security to implement appropriate measures to reduce physical security risks to reasonably acceptable levels while ensuring that properly authorized access is allowed.

3. The Security Officer will consult, as necessary, with the appropriate experts and consultants such as electrical engineers, HVAC technicians, utilities representatives, town officials, etc., regarding physical security and the protection of ePHI on assets.

4. To support the above steps, the Security Officer will document in a Facility Security Plan:

    a) The physical location of all of information systems, programmed equipment and devices that store ePHI.

    b) The physical security measures that exist, for example:

        i) Fire Extinguishers and Suppressant Measures;

        ii) Climate Control Measures;

iii) Door Locks (physical/electronic);

iv) Surveillance Systems; and

v) ID Badges.

5. The Security Officer is responsible for ensuring that the physical security risk to all information systems that contain ePHI is monitored throughout the year.

6. The Security Officer is responsible for conducting a physical security risk audit no less than once per year.

7. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to the extent necessary to accomplish the tasks described in this Policy.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Facility Access Controls – Facility Access Control and Validation Policy

PURPOSE:

To safeguard the physical facilities and software programs and that store, access, retrieve, or transmit ePHI by controlling and validating access to facilities and programs and preventing unauthorized access to Child Health and Development Institute's programs and facilities.

POLICY:

It is the policy of CHDI to establish and implement procedures that will control, validate and prevent unauthorized access to the physical facilities and software programs that access, store, retrieve, or transmit ePHI, including workforce and visitor control procedures.

PROCEDURES:

1. The Security Officer is responsible for identifying and documenting all areas of the physical facilities that house information systems, equipment, programs, or devices that access, store, retrieve, or transmit ePHI. The Security Officer maintains such documentation. In light of the fact that CHDI outsources the facilitation and hosting of the technological infrastructure that maintains all ePHI with a vendor(s), the Security Officer will be responsible for checking-in with the vendor(s) of such infrastructure and ensuring that it has a reasonable and appropriate process for protecting the facilities that house the servers and/or any systems that maintain CHDI's ePHI. With respect to other areas that house information systems or devices (such as CHDI's office space in which computer(s) are located, the Security Officer shall take the lead on compliance with the provisions described below in this Policy.

2. Any authorization of new, temporary, or replacement access badges, key cards, keys, etc. that allow entry into limited or restricted access areas are done in writing, except during an emergency.

3. The Security Officer is responsible for maintaining a log of all keys/access badges that have been issued.

4. The loss of an access badge and/or keys should be reported to the Security Officer at the earliest possible opportunity.

5. All visitors that will access secured areas must be accompanied by an authorized escort.

6. Emergency access to secured areas will be approved by the Security Officer. All emergency access to secured areas must be escorted and supervised.

7. Access codes are changed and locks are re-keyed at the discretion of the Security Officer when a change in workforce occurs, a key or access card has been lost, or at any other time established by the Security Officer.

8. Keys are inventoried routinely and any discrepancies may lead to re-keying, as determined by the Security Officer.

9. All workforce members should report suspected facility security breaches to the Security Officer.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Facility Access Controls – Facility Maintenance Records Policy

PURPOSE:

To safeguard the physical facilities and the assets therein, including information systems, programs, equipment, devices, etc. that store ePHI, from compromise, tampering, and theft, by documenting all repairs, maintenance, and modifications to components of the facility that relate to physical security.

POLICY:

To establish and implement procedures that will document all repairs, maintenance, and modifications to components of the facility that relate to physical security.

PROCEDURES:

1. Prior to performing facility maintenance services, workforce members, repair and maintenance technicians, and outside contractors are educated about the HIPAA Security Rule's standards that pertain to the physical facility and the need to keep accurate maintenance records.

2. Workforce members must document their requests for service and maintenance. Copies of appropriate work orders, technician/service rep service reports, etc. must be attached to all maintenance request forms upon completion of the work. All documentation or a copy thereof shall be sent to the Security Officer.

3. The Security Officer is responsible for keeping a log of all maintenance requests and work completion reports related to physical security.

4. The Security Officer periodically reviews the documentation pertaining to such maintenance records.

5. If a repair/maintenance project has changed the physical facility compliance state, the Risk Assessment is updated by the Security Officer.

6. All records relating to facility security maintenance are retained for seven (7) years.

7. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with

CHDI's vendor to ensure that vendor adequately safeguards the physical facilities containing ePHI that are within vendor's control.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Workstation Use - Workstation Use Policy

PURPOSE:

To ensure that Child Health and Development Institute minimizes the risk of unauthorized access to or disclosure of ePHI, and to prevent the compromise of CHDI's electronic resources that are used to create, store, access, receive or transmit ePHI.

DEFINITIONS:
Electronic resources are computing and telecommunications devices that can execute programs or store data which may include but are not limited to computers, mobile computing devices, smartphones, and storage devices (USB or otherwise connected).

POLICY:

It is the policy of CHDI to implement proper workstation use and security procedures that ensure the security of ePHI.

This policy applies to all forms of confidential electronic data maintained or transmitted by CHDI. CHDI workforce members must report to the CHDI Security Officer any suspected or known unauthorized data modification or destruction.

PROCEDURES:

1. Proper workstation use is a key element in the awareness and training program for all new and existing workforce members.

2. All workforce members should log off any information system if they leave the information system for 60 minutes.

3. Automatic logoff or screen saver activation protects protected health information from being viewed by unauthorized individuals when users are not actively using their computers. Screen savers must be set to activate after three (3) minutes of inactivity. For computers located in highly visible areas, as determined by the Security Officer, the "on resume, password protect option" must be activated to require users to enter his/her password to unlock the screen saver. A user's screen saver password should be the same as the password used to log onto the computer, however if a user does not use a password to log into a computer, then such user can set a screen saver password.

4. Workforce members must not load unauthorized software onto any desktop, workstation, or notebook computers without express permission of the Security Officer.

5. Workforce members must not store ePHI on a local hard drive without the express permission of the Security Officer.

6. Workforce members must store ePHI on a network drive whenever one is available or as directed by the Security Officer.

7. In the event the Security Officer permits ePHI on a local hard drive, workforce members are required to backup all ePHI stored on their local hard drive in accordance with the Data Backup Policy.

8. Workforce members can use desktops, workstation or notebook computers for business only to perform the workforce members' job function.

9. Workforce members cannot use CHDI's desktop, workstation, or notebook computers for personal gain.

10. Workforce members cannot use desktop, workstation, or notebook computers to access ePHI for which they are not authorized.

11. Workforce members who own a desktop, workstation or notebook computer at home cannot store ePHI belonging to CHDI.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Workstation Use - Workstation Security Policy

PURPOSE:

To ensure that Child Health and Development Institute minimizes the risk of unauthorized access to or disclosure of ePHI, and to prevent the compromise in any way of desktop, workstation, and notebook computers that are used to create, store, access, receive, or transmit ePHI.

POLICY:

It is the policy of CHDI to implement procedures that ensure the security of ePHI by controlling access to desktop, workstation, and notebook computers; ensuring that desktop, workstation, and notebook operating systems allow for secure log-in; and allowing for a secure unattended mode (automatic logoff or secure screensaver). Desktop, workstation, and notebook computers will be protected from threats (e.g. malware, flood damage, fire, power surges), patched appropriately, and configured to minimize the unauthorized disclosure of ePHI and the installation of unauthorized software.

1. The Security Officer maintains documentation of the location, status, responsible workforce member, configuration, and other security attributes of each of the Corporation's desktop, workstation, and notebook computers that store ePHI. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to the extent necessary to obtain information necessary to meet this requirement.

2. The Security Officer is responsible for ensuring that the physical placement of all desktop, workstation, and notebook computers that store PHI are:

    a. Placed such that damage from flood, fire, and other hazards is minimized;

    b. Physically secured; and

    c. Situated such that casual observance of ePHI on their screens/monitors is minimized.

3. The Security Officer is responsible for ensuring that the desktop, workstation, and notebook computers that store ePHI:

a. Are running an operating system that allows for:

   i. Secure log-in;

   ii. Automatic Logoff or Secure Screensaver; and

   iii. Encryption where required by the Risk Assessment.

b. They have had all non-essential devices removed or disabled.

c. They have had all necessary operating system patches, updates, and service packs applied.

d. They are running appropriate anti-virus and anti-spyware software.

e. They are free from all forms of malware.

f. No ePHI is stored on them if a network drive is available.

g. Any ePHI that is stored on them is backed up in accordance with CHDI's Backup Policy.

h. Any ePHI that is stored on them is encrypted in accordance with CHDI's Encryption Policy.

i. Other measures as determined by the Risk Assessment

4. In situations where ePHI resides on local hard drives, those drives must be backed up in accordance with CHDI's backup policy.

5. Desktops, workstations, and notebooks that are not owned by CHDI will not be used to create access, store, or transmit ePHI, and will not be placed on CHDI's network for any purpose.

6. The Security Officer is responsible for ensuring that desktop, workstation, and notebook computer information system activity logs and audit trails are reviewed for compliance with this Policy. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to the extent necessary to obtain such information.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Device and Media Controls – Device Disposal Policy

PURPOSE:

To ensure that Child Health and Development Institute implements procedures to address the final disposition of ePHI and/or the hardware or electronic media on which ePHI is stored.

POLICY:

It is the policy of CHDI to control and manage the final disposition of all hardware and/or electronic media on which ePHI is stored by implementing the following procedures.

PROCEDURES:

1. CHDI keeps an inventory of all equipment, devices, or electronic media on an as-needed basis.

2. CHDI contracts with a third-party vendor to ensure that all equipment, devices, and electronic media are sanitized before final disposal. The Security Officer is responsible for ensuring that all hardware and/or electronic media, including portable media, is sanitized prior to transfer to a disposal service. Without limiting this requirement:

    a. The Security Officer is responsible for ensuring that the third-party vendor is using a method of disposal that is appropriate for the type of media in question.

    b. The Security Officer is responsible for ensuring that all hardware and/or electronic media, including portable media, is sanitized prior to transfer from the custody of CHDI to a disposal service.

3. All hardware and/or electronic media, including portable media, that is no longer in use, is not planned for re-use, but has not been transferred must be sanitized before going to storage.

4. The Security Officer is responsible for maintaining a list of all used and stored hardware and/or electronic media, including portable media, to ensure control over the location of hardware and/or electronic media.

5. Any hardware or electronic media sent out for repair or service must be returned, even if it is being replaced.

6. The method of sanitization used by CHDI prior to transfer to the Vendor will be to backup all files to an appropriate folder on the network; then to "select all" and "delete." The CHDI Office Manager and/or HIPAA Security Officer shall ensure that any device/media shows no files prior to transfer to the Vendor for sanitation. The method of sanitization used by the Vendor will depend upon the type of hardware and/or electronic media, and the sensitivity level of the ePHI that is stored on it. Acceptable methods include:

    a. Writing over the hardware and/or media with a commercial utility designed to sanitize media is the preferred method.

    b. Only when that method is not possible or is deemed impractical by the Security Officer should other methods be used, including multiple low-level reformats.

7. An attempt must be made to sanitize any hardware or electronic media deemed to be damaged and inoperable. In the event it is impossible to sanitize the hardware and/or electronic media, it must be physically dismantled and rendered useless.

8. Portable media, such as floppy disks, zip disks, CD-ROMs, backup tapes, etc. that remains in use must be kept physically secure and must be inventoried.

9. Valid Business Associate Agreements must be in place before any outside service provider or consultant can repair or service any hardware and/or electronic media that stores ePHI, or pick up hardware and/or electronic media for commercial disposal.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Device and Media Controls – Media Re-Use/Transfer Policy

PURPOSE:

To ensure that Child Health and Development Institute implements procedures to address the removal of ePHI from hardware and/or electronic media before it is made available for re-use.

POLICY:

It is the policy of CHDI to control and manage all hardware and/or electronic media that stores ePHI and is identified for re-use in order to minimize the risk of unauthorized disclosure of ePHI.

PROCEDURES:

1. The Security Officer is responsible for documenting the transfer of all hardware and/or electronic media for the purpose of re-use.

2. The Security Officer will decide which equipment and/or electronic media transferred within CHDI for re-use may require sanitization, based upon the ePHI stored on the hardware and/or electronic media and the authorization level of the user that the hardware and/or electronic device is being transferred to for re-use.

3. If the hardware and/or electronic media transferred within CHDI is deemed "must sanitize", then it must be sanitized in a manner consistent with the HIPAA Security Rule Device Disposal Policy.

4. The Security Officer's decision regarding the sanitization of hardware and/or electronic media for re-use will be documented by the Security Officer.

Child Health and Development Institute
Effective Date: July 1, 2014

— ADDRESSABLE —

SUBJECT: Device and Media Controls - Accountability Policy

PURPOSE:

To ensure that Child Health and Development Institute implements procedures to control and manage the movements of hardware and/or electronic media that stores ePHI.

POLICY:

It is the policy of CHDI to document and report upon the movement of all hardware and/or electronic media that stores ePHI in order to minimize the risk of unauthorized disclosure of ePHI.

PROCEDURES:

1. The Security Officer will appoint media custodians, as necessary, for hardware and/or electronic media, including portable media that stores ePHI. The media custodians will be responsible for maintaining a log of the movements of the media for which media custodians are responsible and for submitting such logs to the Security Officer.

2. The Security Officer will review the appropriate logs periodically, but no less than once per year.

Child Health and Development Institute
Effective Date: July 1, 2014

-ADDRESSABLE-

SUBJECT: Device and Media Controls – Data Backup and Storage Policy

PURPOSE:

To protect the integrity and availability of ePHI by implementing procedures to make an exact retrievable copy of ePHI prior to moving or transferring equipment, devices, and/or other electronic media that stores ePHI.

POLICY:

It is the policy of Child Health and Development Institute to make an exact retrievable copy of ePHI prior to moving or transferring equipment, devices, and/or other electronic media that stores ePHI.

PROCEDURES:

1. CHDI contracts with a third-party vendor to store and maintain all electronic data, including ePHI, on CHDI's behalf. CHDI prohibits the storage of any ePHI on anything other than the electronic system that is stored and maintained by such third-party vendor. CHDI shall ensure that such third-party vendor will backup all data, including ePHI, on a regular basis.

2. CHDI will ensure that all vendors perform data backups and destroy such data (when necessary) in accordance with HIPAA Security Rule requirements.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Access Control - Unique User Identification Policy

PURPOSE:

The purpose of this policy is to ensure that all individuals who access ePHI are identified by a unique user ID and are authenticated via a unique password or other authentication mechanism.

POLICY:

It is the policy of CHDI to allow users access to ePHI only via a unique user ID and authentication mechanism such as a unique password.

PROCEDURES:

1. The Security Officer adheres to a system for granting access to information systems. This system includes the:

    a) Assignment of a unique user ID,

    b) Assignment of rights attached to the unique user ID, and

    c) Assignment of a unique password or some other authentication method.

2. Access to any information system that receives, stores, transmits, or accesses ePHI shall be via a unique user ID and one or more forms of authentication, such as the entering of a unique password or the use of a biometric device.

3. Training and reminder programs shall include instruction for users regarding unique user IDs and passwords. The instruction shall include:

    a) Users may only access the information systems via a user ID that has been assigned to him/her.

    b) Users must not share their user IDs and passwords with anyone else.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Access Control – Emergency Access Policy

PURPOSE:

To ensure that Child Health and Development Institute implements procedures to provide access to critical systems that receive, store, transmit, or access ePHI during an emergency situation.

POLICY:

It is the policy of CHDI to provide access to critical systems that receive, store, transmit, or access ePHI during emergency situations by implementing the following procedures.

PROCEDURES:

The ePHI that is maintained by CHDI is information that is received by CHDI from another party. CHDI is never the original source of the ePHI. Such ePHI is duplicative and maintained by another entity (covered entity or business associate). As such, the ePHI maintained by CHDI is not critical in nature and it is highly unlikely that any individual/entity would go to CHDI to obtain a copy of such information in an emergency. Notwithstanding the foregoing, the Security Officer will ensure that any vendor maintaining ePHI will have processes for accessing all ePHI in an emergency. The Security Officer will detail the processes and methods involved in accessing the information systems during an emergency situation in the Disaster Recovery Plan.

Child Health and Development Institute
Effective Date: July 1, 2014

-ADDRESSABLE-

SUBJECT: Access Control – Automatic Logoff Policy

PURPOSE:

To ensure that Child Health and Development Institute implements electronic procedures that terminate an electronic session after a predetermined time of inactivity.

POLICY:

It is the policy of CHDI to ensure that CHDI implements electronic mechanisms that terminates an electronic session after a predetermined time of inactivity.

PROCEDURES:

1. The Security Officer will ensure that CHDI's systems that receive, store, transmit, or access ePHI, which are located in open-access or public areas, implement some form of automatic logoff functionality.

2. The Security Officer will instruct workforce members to utilize the automatic logoff feature of their systems and applications that have the feature, and will set the logoff period commensurate with the organization's policies.

3. The Security Officer will ensure that systems and applications that do not allow for automatic logoff reside on an operating system that does. The Security Officer will ensure that the operating system's automatic logoff feature is implemented.

4. The Security Officer will periodically monitor and test that the automatic logoff methods in place are being used properly.

Child Health and Development Institute
Effective Date: July 1, 2014

-ADDRESSABLE-

SUBJECT: Access Control – Encryption & Decryption Policy

PURPOSE:

To protect against the unauthorized disclosure of ePHI by implementing a mechanism to encrypt and decrypt ePHI.

POLICY:

It is the policy of Child Health and Development Institute to encrypt and decrypt certain ePHI prior to electronic transmission in order to protect against the unauthorized disclosure of that ePHI.

PROCEDURES:

1. All ePHI that is being electronically transmitted must be transmitted via a process that encrypts the ePHI prior to transmission.

    a. To encrypt ePHI prior to transmission via email, all users must insert the word "[secure]" (with the brackets before and after the word "secure") in the subject line. This will trigger the system to automatically encrypt the email prior to transmitting it to the recipient; or

    b. Select the "Secure Lock" icon to ensure encryption of the message.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Audit Controls - Audit Controls Policy

PURPOSE:

The purpose of this policy is to record and examine information system activity.

POLICY:

It is the policy of CHDI to implement and utilize the hardware, information systems, applications, and procedural measures to record and report upon information system activity in information systems that receive, store, transmit, or otherwise access ePHI and to examine and review recorded activity on a periodic basis and to maintain and store such recorded activity for a reasonable amount of time.

PROCEDURES:

1. The Security Officer is responsible for ensuring that the appropriate workforce members in charge of information systems, applications, or devices that receive, store, transmit, or otherwise access ePHI are educated on the features and functionality of their systems that relate to audit controls.

2. The Security Officer is responsible for ensuring that the appropriate audit control features that are available are turned "on" and utilized in all information systems, applications, and devices that receive, store, transmit, or otherwise access ePHI.

3. The Security Officer is responsible for determining what information needs to be captured by audit control features and functionality.

4. The Security Officer is responsible for determining:

    a) Which audit control reports must be generated from each information system, application and device;

    b) How often they should be generated and in what manner;

    c) Who shall receive and review the audit control information, when, and how;

    d) Procedures for documenting and reporting audit control discrepancies;

e) The length of time and manner in which to store the generated audit control information and make the information available to the audit team;

f) The manner in which to purge the generated audit control information.

5. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to accomplish the purpose of this Policy.

Child Health and Development Institute
Effective Date: July 1, 2014

-ADDRESSABLE-

SUBJECT: Integrity – Mechanism to Authenticate ePHI Policy

PURPOSE:

To ensure that transmitted ePHI is not improperly modified or destroyed without detection in an unauthorized manner until it is disposed of.

POLICY:

It is the policy of Child Health and Development Institute to implement electronic measures and mechanisms to ensure that ePHI is not improperly modified or destroyed without detection in an unauthorized manner until it is disposed of.

PROCEDURES:

1. The integrity of ePHI can be compromised, among other ways, when ePHI is being restored into an information system, during an information system conversion, or during a technical support session by a vendor. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to ensure that the information system(s) have appropriate electronic mechanisms and measures to prevent the improper modification or destruction of ePHI. The Security Officer is responsible for ensuring that the foregoing integrity controls are documented in the Risk Assessment.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Person or Entity Authentication - Person/Entity Authentication Policy

PURPOSE:

To ensure that Child Health and Development Institute implements procedures to verify that a person or entity seeking access to ePHI via an information system is the one claimed.

POLICY:

It is the policy of CHDI to verify that a person or entity seeking access to ePHI via an information system must be the one claimed by implementing the following procedures.

PROCEDURES:

1. The Security Officer is responsible for ensuring that access to any information system, application or device is only granted through the use of a unique user ID and password.

2. Remote access to ePHI is only allowed on an information system that can authenticate users.

3. Permission to email or otherwise transmit ePHI is only granted after reasonable attempts have been made to authenticate the recipient.

Child Health and Development Institute
Effective Date: July 1, 2014

-ADDRESSABLE-

SUBJECT: Transmission Security - Transmission Integrity Controls Policy

PURPOSE:

The purpose of this policy is to ensure that transmitted ePHI is not improperly modified or accessed without detection until it is disposed of.

POLICY:

It is the policy of CHDI to implement electronic measures and mechanisms to ensure that ePHI is not improperly modified or accessed without detection until it is disposed of. To protect ePHI transmission from one point to another in a manner commensurate with the associated risk.

PROCEDURES:

1. In light of the fact that CHDI outsources the facilitation and management of its information technology systems, the Security Officer will work with CHDI's vendor to ensure that the security and integrity of ePHI is protected.

2. The Security Officer is responsible for ensuring that the transmission processes are documented in the Risk Assessment.

Child Health and Development Institute
Effective Date: July 1, 2014

-ADDRESSABLE-

SUBJECT: Transmission Security - Transmission Encryption Policy

PURPOSE:

The purpose of this policy is to ensure that transmitted ePHI is encrypted whenever it is deemed appropriate to commensurate with the associate risk.

POLICY:

It is the policy of CHDI to encrypt transmitted ePHI whenever it is deemed appropriate commensurate with the associated risk.

PROCEDURES:

1. The Security Officer shall determine and document the situations in which ePHI is transmitted.

2. The Security Officer shall determine the appropriate measures and mechanisms necessary to protect ePHI during the transmission process for each transmission situation. The measures and mechanisms must be commensurate with the risk-level of the ePHI being transmitted and the situation.

3. All high-risk ePHI being transmitted must be protected by an encryption measure.

4. The measures and mechanisms used to protect ePHI that is not high-risk must be thoroughly documented, if those measures and mechanisms do not include encryption.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: HIPAA Security Rule Recordkeeping Policy

PURPOSE:

The purpose of this policy is to ensure that CHDI complies with applicable rules regarding the maintenance of records required by the HIPAA Security Rule.

POLICY:

It is the policy of CHDI to maintain records required for compliance with the HIPAA Security Rule for the period required by law.

PROCEDURES:

1. **Documentation**. CHDI must maintain:

    a. HIPAA Security Rule policies and procedures in written or electronic format; and

    b. A written or electronic record of any action, activity or assessment required by the Security Rule to be documented.

2. **Retention**. CHDI must maintain all documentation for a period of six years from the date of its creation or the date when it was last in effect, whichever is later.

3. **Availability**. CHDI must make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

4. **Updates**. CHDI will periodically review these policies and procedures and update these policies and procedures as needed in response to environmental or operational changes affecting the security of ePHI.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Use and Disclosure of Protected Health Information Subject to the Minimum Necessary Requirement Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws that require CHDI to make reasonable efforts to limit protected health information used, disclosed, or requested to the minimum necessary for the intended purpose.

POLICY:

It is the policy of CHDI that when using, disclosing, or requesting protected health information, CHDI will limit such protected health information, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

PROCEDURES:

1. **Minimum Necessary**.

   a. *When Minimum Necessary Standard Applies.* When using or disclosing protected health information or when requesting protected health information from another entity, CHDI will limit such protected health information, to the extent practicable, to the limited data set (as defined in Section 2 below) or, if necessary to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request, unless an exception specified below is applicable.

   b. The following uses and disclosures that apply at CHDI are exempt from the minimum necessary requirement:

      i. Uses or disclosures made to an individual who is the subject of the protected health information;

      ii. Uses or disclosures made pursuant to an authorization;

      iii. Disclosures made to the Secretary of the United States Department of Health and Human Services; and

      iv. Uses or disclosures that are required by law.

c. When disclosing protected health information, CHDI shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

2. **Contents of Limited Data Set.** A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

a. Names;

b. Postal address information, other than town or city, State or zip code;

c. Telephone numbers;

d. Fax numbers;

e. Electronic mail addresses;

f. Social security numbers;

g. Medical record numbers;

h. Health plan beneficiary numbers;

i. Account numbers;

j. Certificate/license numbers;

k. Vehicle identifiers and serial numbers, including license plate numbers;

l. Device identifiers and serial numbers;

m. Web Universal Resource Locators (URL's);

n. Internet Protocol (IP) address numbers;

o. Biometric identifiers, including finger and voice prints; and

p. Full face photographic images and any comparable images.

3. **Compliance with Department of Health and Human Services Guidance on Minimum Necessary**. When guidance to be issued by the Secretary as to what constitutes "minimum necessary" becomes effective, CHDI will follow such guidance, as applicable, in using, disclosing, and requesting protected health information.

Child Health and Development Institute
Effective Date: July 1, 2014

SUBJECT: Accounting of Disclosures of Protected Health Information Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable laws that grant individuals or an individual's legal representative (collectively referred to herein as the "individual") the right to request an accounting of certain disclosures of protected health information.

POLICY:

It is the policy of CHDI that CHDI will only maintain identifiers that are considered part of a limited data set. As such, HIPAA exempts limited data sets from the accounting of disclosure requirements. In light of the foregoing, CHDI does not track accounting of disclosures. In the event that CHDI maintains more than a limited data set of PHI, it will comply with the procedures set forth below.

PROCEDURES:

1. **Disclosures Which Must Be Accounted For**. Individuals have a right to receive an accounting of disclosures of protected health information made by CHDI in the six (6) years prior to the date on which the accounting is requested, except for disclosures:

    a) To carry out treatment, payment or health care operations, unless as of January 1, 2011 these disclosures are made through a covered entity's electronic health record, in which case the accounting for treatment, payment, and health care operations disclosures is limited to the three (3) years preceding the request;

    b) To the individual about his or her own information;

    c) Pursuant to an authorization;

    d) For national security or intelligence purposes as permitted under law;

    e) To correctional institutions or law enforcement officials as permitted under law;

    f) That are the responsibility of the applicable covered entity to account for, pursuant to the Business Associate Agreement between such covered entity and CHDI. In such event, CHDI shall make available to the covered entity the information pertaining to

CHDI's disclosures, if any, required by the covered entity to provide an accounting of disclosures to an individual. Any questions with respect to the responsibility of CHDI to provide an accounting of disclosures should be directed to the Security Officer.

g) That occurred prior to February 17, 2010. The applicable covered entity shall be responsible for responding to requests for accountings of disclosures that occurred prior to February 17, 2010, and CHDI shall make available to the covered entity the information pertaining to CHDI's disclosures, if any, required by the covered entity to provide such an accounting to an individual.

h) That occurred prior to January 1, 2011, with respect to disclosures made from a covered entity's electronic health record; provided, however, that a later date may be applicable, depending on when the covered entity on whose behalf disclosures were made acquired the electronic health record. Any questions with respect to the timeframe applicable to an individual's right to receive an accounting of disclosures made from a covered entity's electronic health record should be directed to the Security Officer.

i) Which would impede health oversight or law enforcement activities. The accounting for disclosures of protected health information to a health oversight agency or law enforcement official must be suspended for the time period specified by such agency or official if the agency or official provides a written statement asserting that the provision of an accounting would be reasonably likely to impede the activities of the agency or official and specifying a time period for the suspension. If oral notification by a health oversight agency or law enforcement official is given, such notification must be documented, including the identity of the agency or official making the request and suspend the individual's right to an accounting of disclosures for no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted by the agency or official during that time period.

2. **Disclosures of protected health information containing HIV-related information**. Connecticut law requires that an accounting of all disclosures of HIV-related information be maintained, unless the disclosure was made to:

a) A federal, state, or local health officer when the disclosure is authorized by Connecticut or Federal law; or

b) Persons reviewing information or records in the ordinary course of ensuring that a health facility is complying with applicable quality

of care standards; program evaluation; program monitoring; or service review.

There is no right of law enforcement or a health oversight agency to unilaterally suspend the provision of an accounting of HIV-related information.

3. **Maintaining an Accounting**. A written accounting of certain non-routine disclosures of protected health information shall be maintained (in accordance with Section 1 above) and an electronic accounting of disclosures made through the covered entity's electronic health record for such non-routine disclosures and for disclosures for treatment, payment, and health care operations shall be maintained, as required by Connecticut and Federal law.

4. **Responding to a Request for an Accounting**.

   a) Determination of Responsibility to Respond to a Request for an Accounting: If an individual receives CHDI's contact information directly from a covered entity and requests an accounting of disclosures from CHDI, CHDI shall respond to the request in accordance with this policy, unless the Business Associate Agreement between CHDI and the applicable covered entity specifies that the covered entity will be responsible for providing an accounting of disclosures made by CHDI on behalf of the covered entity. Questions with respect to the responsibility to respond to a request for an accounting of disclosures should be directed to the Security Officer.

   b) Oral Request for an Accounting: If an individual orally requests an accounting of their protected health information, such individual will be given a Request for Accounting of Disclosures form (sample attached). The Request form must be completed, signed and dated by the individual.

   c) Written Request for an Accounting: If an individual submits a written request for an accounting, the Security Officer will determine whether the request is adequate based on the information provided.

   d) Incomplete Requests: If the individual's request for an accounting is incomplete, CHDI will send the individual a written Notice of Accounting Denial form (sample attached) requesting necessary outstanding information so that the request can be processed.

5. **Determining Right to an Accounting**: The Security Officer shall determine whether a request for an accounting should be granted or denied

for reasons acceptable under Connecticut and Federal law. Such determination will be made within the applicable timeframes.

a) Notice of Extension of Time: In the event that an individual's request for an accounting cannot be responded to within the applicable timeframe, the Security Officer shall send the individual a Notice of Extension of Time form (sample attached). An extension of time may only be issued to an individual on one occasion per request for an accounting.

6. **Granting a Request for an Accounting**:

a) Fees for the Accounting: The Security Officer will determine whether the individual has requested more than one accounting within a twelve-month period. If so, the Security Officer shall determine the fee to be imposed, if any, for the accounting. If a fee will be imposed, CHDI will send a Notice of Fee for Accounting form (sample attached) to the individual.

b) Written Notice: If the Security Officer determines that an Individual's request for an accounting will be granted and the accounting is in response to the first request for an accounting within a twelve-month period, any fee associated with the accounting has been waived, or the individual has agreed to any fee, CHDI will complete and send the individual an Accounting of Disclosures form (sample attached).

7. **Denying a Request for an Accounting**: If the Security Officer denies the individual's request for an accounting, CHDI shall send the individual a Notice of Accounting Denial form (sample attached).

8. **Content Requirements**

a) The written accounting of disclosures, other than disclosures through a covered entity's electronic health record (addressed in Section 8(b) below), must meet the following requirements:

i) The accounting must include the disclosures of protected health information that occurred during the six (6) years (or less as specified in the request) prior to the date of the request (but after April 14, 2003), including disclosures by or to agents and subcontractors of CHDI;

ii) The accounting of each disclosure must include:

(A) Date of disclosure;

(B) Name of entity or person who received the protected health information, and, if known, the address of such entity or person;

(C) A brief description of the protected health information disclosed;

(D) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of a statement, a copy of the written request for disclosure.

(E) Multiple Disclosures:

If, during the time period for the accounting, multiple disclosures have been made to the same entity or person for a single purpose, the accounting may provide the information as set forth above for the first disclosure, and then summarize the frequency, periodicity, or number of disclosures made during the accounting period and the date of the last such disclosure during the accounting period. (Sample Multiple Disclosures Form is attached.)

For HIV-related information all disclosures must be included in the accounting (even multiple disclosures to a single person or entity for a single purpose), except for multiple disclosures made to government agents who require information necessary for payments to be made on behalf of individuals pursuant to contract or law, which may be accounted for as set forth above.

b) Effective January 1, 2011, the accounting of disclosures through the applicable covered entity's electronic health record, including disclosures for treatment, payment, and health care operations, and including disclosures by or to CHDI's agents and subcontractors, must meet the following requirements:

i) The accounting must include the disclosures of protected health information that occurred during the three (3) years (or less as specified in the request) prior to the date of the request;

ii) The accounting of each disclosure must include those elements specified in Section 8(a)(ii) above.

9. **Provision of the Accounting**.

a) Timing: If an individual requests an accounting, CHDI must act on such request no later than sixty (60) days after receipt of such a request. In the event CHDI is unable to provide the accounting within sixty (60) days, CHDI may extend the time to provide the accounting by no more than thirty (30) days if CHDI provides the individual with a written statement of the reasons for the delay and the date by which CHDI will provide the accounting.

b) Fees: The first accounting in any twelve-month period must be provided to the individual without charge. A reasonable, cost-based fee may be charged for additional accountings within the twelve-month period, provided the individual is informed in advance of the fee, and is permitted an opportunity to withdraw or amend the request.

10. **Documentation**. CHDI shall retain documentation, in written or electronic format, of all written accountings provided to the individual.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Notification of Breach of Protected Health Information Policy

PURPOSE:

The purpose of this policy is to ensure that Child Health and Development Institute complies with applicable state and federal law regarding notice of breach of protected health information.

POLICY:

It is the policy of CHDI to provide notification of breach of unsecured protected health information in accordance with the procedures set forth below. The Security Officer shall coordinate and oversee CHDIs obligations pursuant to this policy.

DEFINITIONS:

"Breach" means the unauthorized acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA privacy regulations and that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

1. The term "breach" does not include:

    a) any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of CHDI if:

        i) Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with CHDI; and

        ii) Such information is not further acquired, accessed, used, or disclosed by any person.

    b) Any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by CHDI to another similarly situated individual at the same facility, and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed in a

manner not permitted under the HIPAA privacy regulations by any person.

c) A disclosure of PHI where CHDI has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

d) Except as specifically excluded from the definition of a "breach," an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA privacy regulations is presumed to be a breach unless the Corporation demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(ii) the unauthorized person who used the PHI or to whom the disclosure was made;

(iii) whether the PHI was actually acquired or viewed; and

(iv) the extent to which the risk to the PHI has been mitigated.

"Unsecured protected health information" means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services. The Security Officer shall determine whether any breach involves unsecured protected health information.

PROCEDURES:

1. **Discovery of a Breach of PHI**.

a. All workforce members are responsible for immediately reporting an actual or suspected breach of protected health information, whether secured or unsecured, to the Security Officer.

b. A breach is treated as discovered as of the first day on which such breach is known to the Corporation or, by exercising reasonable diligence, would have been known to the Corporation.

c. The Security Officer will receive, document, and investigate all actual or reasonably suspected breaches of protected health information in a timely manner in accordance with this policy.

2. **Determining Whether a Breach Has Occurred**

a) Determining Impermissible Use or Disclosure. To determine whether a breach of protected health information has occurred, the Security Officer will first determine whether the incident involved an impermissible use or disclosure of protected health information that would violate the HIPAA Privacy Rule.

b) Determining Whether Unsecured Protected Health Information was Involved. If it is determined that the incident involved an impermissible use or disclosure of protected health information, the Security Officer will then determine whether the incident involved secured or unsecured protected health information. If the incident did not involve unsecured protected health information, the notice requirements set forth below do not apply. The Security Officer will, however, work with staff and others as appropriate to mitigate any harmful effect of the incident to the extent practicable, in accordance with applicable policies and procedures.

c) Determining Whether an Exception to the Definition of Breach Applies. The Security Officer will determine whether an incident involving unsecured protected health information falls under one of the exceptions to the definition of breach, as specified in the Definitions section above. If an exception applies, the incident would not constitute a breach, and the Security Officer will document such determination. If the incident did not involve a breach, the notice requirements set forth below do not apply.

d) Determining Whether there is a Low Probability that the Protected Health Information has been Compromised. If it is determined that the incident involved an impermissible use or disclosure of unsecured protected health information, and an exception to the definition of breach does not apply, the Security Officer will perform a risk assessment to determine whether there is a low probability that the PHI has been compromised. The Security Officer will at a minimum consider the required factors outlined above and document such risk assessment. In addition to consideration of the *required* factors, the Security Officer may consider additional factors to appropriately assess whether the PHI has been compromised. If the risk assessment does not demonstrate that there is a low probability that the PHI has been compromised, the incident will constitute a breach and CHDI will comply with the notice requirements set forth below. If, however, it is determined that there is a low probability that the PHI has been compromised, then there is no breach.

e) Documentation. The Security Officer is responsible for maintaining documentation of (i) all required notifications that were made as provided in this policy, (ii) all assessments performed in determining whether a breach has occurred and the outcomes of such assessments, including whether an impermissible use or disclosure of protected health information satisfied an exception to the definition of breach.

3. **Notification of Breach to Covered Entities**.

a. *General Notification Requirement*. In the event that CHDI discovers a breach of unsecured protected health information, CHDI shall notify the covered entity of such breach.

b. *Content of Notification.* Notice of breach provided to the covered entity shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by CHDI to have been, accessed, acquired, or disclosed during such breach. The covered entity will also be provided with any other available information as it becomes available that covered entity is required to include in the notification to the individual under 45 C.F.R. § 164.404(c), either at the time it provides notice to the covered entity of the breach or promptly thereafter as information becomes available

c. *Notification Timeframe.* CHDI shall make notification to the covered entity in accordance with the timeframe specified in CHDI's business associate agreement with the covered entity. In the event that no timeframe is specified, then such notification shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by CHDI. CHDI will provide the covered entity with the information required under the Content of Notification section of this Policy even if it becomes available after notifications have been sent to affected individuals or after the 60-day period (or, if shorter, the applicable timeframe under the business associate agreement with the covered entity) has elapsed.

d. *Delaying the Notification*. If a law enforcement official determines that providing a notification of breach would impede a criminal investigation or cause damage to national security, then the notification of breach will be delayed. If a law enforcement official provides the notification in writing and such notification includes the length of time that the notification must be delayed, then the notification of breach will delayed for the time specified. If the law enforcement official provides such notification orally, then the statement and identity of the official will be documented

and the notification of breach will be delayed no longer than 30 days, unless the law enforcement official provides a written statement as provided above.

4. **State Law Breach Notification Requirements.**
The Security Officer shall consult with CHDI's legal counsel as appropriate to determine whether other state laws regarding data breach notification obligations may apply.

5. **Documentation**. The Security Officer will maintain documentation that (a) all required notifications were made as provided in this policy, (b) the risk assessment revealed that there was a low probability that the PHI has been compromised as a result of the impermissible use or disclosure of PHI, and/or (c) the use or disclosure of PHI satisfies an exception to the definition of breach.

Child Health and Development Institute
Effective Date: November 1, 2015
-REQUIRED-

SUBJECT: Privacy Protection Policy

PURPOSE: The purpose of this policy and procedure is to protect the privacy of confidential information of the Child Health and Development Institute of Connecticut, Inc. ("CHDI") and its clients and to document safeguards for protecting and securing confidential information against loss, destruction, theft, and unauthorized access or removal.

SCOPE: This policy and procedure applies to all CHDI employees and other personnel who provide services on behalf of CHDI.

OVERVIEW: There are three types of information breaches that CHDI is required to protect against: (1) a breach of protected health information under HIPAA; (2) a breach of security of personal information pursuant to Connecticut's computerized data security breach law; and (3) a confidential information breach that relates to confidential information received or created by CHDI pursuant to a state contract. Except as described in this policy, the safeguards that CHDI has implemented to protect the privacy and security of protected health information under HIPAA shall apply to all Covered Information (as defined below).

DEFINITIONS:

"**Breach of Security**" means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing Personal Information (as defined below) when access to the Personal Information has not been secured by encryption or by any other method or technology that renders the Personal Information unreadable or unusable.

"**CHDI Information**" means information about CHDI or its personnel that is deemed confidential or sensitive. CHDI information includes, but is not limited to, financial information, human resources information (such as employee records), business transactions, contracts, and client lists. All personnel should consult with their supervisor or contact the Vice President of Finance & Operations or the HIPAA Secuity Officer if they are unsure whether certain information is confidential.

"**Confidential Information**" means an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation, personal information subject to the federal Family

Educational Rights and Privacy Act of 1974 (as amended from time to time) and protected health information, as defined in the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended from time to time. In addition, "Confidential Information" includes any information that a State Contracting Agency disclosing Confidential Information to CHDI pursuant to a written agreement with CHDI identifies as confidential. "Confidential Information" shall not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records which are lawfully made available to the general public.

"**Confidential Information Breach**" means an instance where an unauthorized person or entity accesses Confidential Information that is subject to or otherwise used in conjunction with any part of a written agreement with a State Contracting Agency in any manner, including, but not limited to, the following occurrences:

(i) any Confidential Information that is not encrypted or secured by any other method or technology that renders the information unreadable or unusable is misplaced, lost, stolen or subject to unauthorized access;

(ii) one or more third parties have accessed, or taken control or possession of, without prior written authorization from the state,

(A) any Confidential Information that is not encrypted or protected, or

(B) any encrypted or protected Confidential Information together with the confidential process or key that is capable of compromising the integrity of Confidential Information; or

(iii) there is a substantial risk of identity theft or fraud of the client of the State Contracting Agency, CHDI, the State Contracting Agency or the State of Connecticut.

"**Covered Information**" means information covered by this policy, i.e. Confidential Information, Personal Information and CHDI Information.

"**Personal Information**" means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (a) Social Security number; (b) driver's license number or state identification card number; or (c) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

"**State Contracting Agency**" means any state agency disclosing confidential information to CHDI pursuant to a written agreement with CHDI for the provision of goods or services to the State of Connecticut.

POLICY: It is the policy of CHDI to ensure that appropriate safeguards exist to protect and keep confidential all Covered Information that CHDI comes to possess or control, wherever and however stored or maintained, and to protect such information from a breach.

PROCEDURE:

A. Storage of and Access to Covered Information

Collection of Covered Information or Personal Information: CHDI will collect Covered Information or Personal Information only when it is necessary for CHDI's operations.

Storage of Covered Information: Individual departments within CHDI shall be responsible for having adequate controls and protections to secure all documents containing Covered Information, whether such Covered Information is in paper form or stored electronically, so as to minimize potential misuse and inappropriate access or disclosure of such information. This includes measures to restrict access to Covered Information and the area where such records are kept. Covered Information should not be left in an unlocked room or unsecure area. Only authorized personnel should have access to Covered Information. The supervisor of each department shall document the controls and procedures that the department has implemented to carry out the requirements of this section and shall maintain a historical record of such controls and procedures, and shall provide a copy to the Vice President of Finance and Operations. The supervisor of each department shall review such controls and procedures annually and update them as appropriate.

Access: CHDI employees are permitted to access and use certain Covered Information only as necessary and appropriate to carry out their assigned tasks in the performance of their respective job functions and, with respect to Confidential Information from a State Contracting Agency, as necessary for completion of the contracted services. Access to Covered Information is based on an individual's job responsibilities. Any employees granted such access must take all necessary precautions to ensure the integrity of records that include Covered Information. With respect to electronic Covered Information, such Covered Information shall be password protected. The access and password protections describe in CHDI's HIPAA policies and procedures shall govern access to Covered Information maintained electronically.

Electronic data constituting Confidential Information obtained from a State Contracting Agency must be maintained: (i) in a secure server, (ii) on secure drives, (iii) behind firewall protections and monitored by intrusion detection software, (iv) in a manner where access is restricted to authorized employees and their authorized agents, and (v) as otherwise required under state and federal law. Unless permitted by an agreement with a State Contracting Agency, (1) CHDI may not store Confidential Information that relates to a contract with a State Contracting Agency on stand-alone computer or notebook hard disks or portable storage devices, such as external or removable hard drives, flash cards, flash drives, compact disks or digital video disks; and (2) CHDI may not copy, reproduce or transmit data constituting Confidential Information, except as necessary for the completion of the contracted services. Any copies of Confidential Information are

subject to the provisions of this policy in the same manner as originals of such Confidential Information.

B. Reporting and Destruction

Reporting: Any employee aware of unauthorized use, access or disclosure of Covered Information must report such activity and/or provide any copies of the Covered Information to their supervisor or to the Vice President of Finance & Operations or the HIPAA Security Officer.

Destruction: Each department is responsible for ensuring that both paper and electronic records which contain Covered Information will be maintained and destroyed in accordance with CHDI's record retention and destruction policies and procedures.

C. Removal and Transportation of Covered Information

Records and other documents containing Covered Information ("records") are the property of CHDI. Records may be removed from CHDI only as required by law or with the permission of the custodian of the records for the applicable location and, if applicable, in accordance with the applicable state contract. The custodian of records for certain categories of information are as follows:

Category	Custodian
Financial records	Vice President of Finance & Operations
Records containing "personal information" or "protected health information"	HIPAA Security Officer
Client Contracts	Vice President of Finance & Operations
Human Resources Records	Vice President of Finance & Operations

Should authorization be granted to remove records, or any component thereof, originals may not be removed. Rather, a copy must be made and the original record must remain on CHDI's premises. Any electronic media containing Covered Information must be backed up before it is moved.

Individuals authorized to remove records are responsible for safeguarding such records from loss, tampering, dissemination, theft, and unauthorized access or use when the records are removed by such individual from the CHDI premises and until the records are properly returned or destroyed. Records must be placed in a bag, envelope, folder, or other appropriate container, or appropriately concealed. The employee or other authorized individual transporting the Covered Information must maintain constant physical possession of the Covered Information. Records should never be left unattended, even temporarily. Records should not be left in unsecured locations, such as an individual's home or car. Records must be transported in a secure, approved manner. Administrators are responsible for supervising and approving transport of Covered Information.

All copies of Covered Information must be tracked prior to removal of the information from a CHDI location. The tracking system must be sufficient to identify the records that have been removed, the types of information contained in such records, the person removing the records, and the date that such records were returned.

When the purpose for removing records has been fulfilled, and the need for removal no longer exists, the individual must return the records to CHDI or properly destroy the records (for example, by finely shredding paper records or, in the case of information stored electronically, by deleting the records from the storage device and performing such other erasure or destruction steps as may be proscribed by the IT department).

Subcontractors or vendors of CHDI may only be granted authorization to remove paper copies of Covered Information once an appropriate agreement, such as a Business Associate Agreement or a confidentiality agreement has been approved by the HIPAA security officer and, if applicable, such removal is permitted by the client contract to which the information relates.

D. Security Awareness and Training

CHDI shall maintain an active and ongoing security awareness and training program. Training is mandatory for all employees who have, or may have, access to confidential information. Such training may be combined with HIPAA training as appropriate, however, any training must, at a minimum, advise employees of the confidentiality of Confidential Information, the safeguards required to protect Confidential Information, and any civil and criminal penalties for noncompliance under federal and state law.

E Breach

All workforce members are responsible for immediately reporting an actual or suspected breach of Covered Information, whether such Covered Information is unencrypted or encrypted, to the Security Officer. Any actual or suspected breach of Covered Information shall be addressed through CHDI's Notification of Breach of Protected Health Information Policy. In the event that such actual or suspected breach involves Confidential Information or Personal Information, additional state notification requirements are set forth below.

Notification of a Confidential Information Breach. If the incident involves Confidential Information that relates to a contract with a State Contracting Agency, then CHDI must notify the State Contracting Agency and the Connecticut Attorney General as soon as practical after CHDI becomes aware of or has reason to believe that such Confidential Information has been subject to a Confidential Information Breach. **The terms of a contract with a State Contracting Agency may require a more specific notification period. For example, The contract may require CHDI to notify a State Contracting Agency no later than twenty-four (24) hours after becoming aware of a Confidential Information Breach. The applicable state contract(s) must be consulted to ensure**

compliance with the applicable reporting obligations. If directed by the applicable State Contracting Agency, CHDI must immediately cease all use of the data provided by such State Contracting Agency or developed internally by the contractor pursuant to a written agreement with the state. CHDI should be prepared to submit to the Office of the Attorney General and the State Contracting Agency either (A) a report detailing the breach or suspected breach, including a plan to mitigate the effects of any breach and specifying the steps taken to ensure future breaches do not occur, or (B) a report detailing why, upon further investigation, the contractor believes that no breach has occurred. *Notification of a Breach of Security of Personal Information.* If the incident is a Breach of Security of Personal Information, then CHDI shall provide notice of the Breach of Security to any resident of the State of Connecticut whose Personal Information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than ninety (90) days after the discovery of such breach, unless a shorter time is required under federal law (e.g. HIPAA), subject to the completion of an investigation to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Notice may be provided in writing, via telephone or electronically, as determined to be appropriate by the Vice President of Finance and Operations and in accordance with applicable law. Notice is not required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, CHDI reasonably determines that the breach will not likely result in harm to the individuals whose Personal Information has been acquired and accessed. Notice required by this section must be delayed for a reasonable period of time if a law enforcement agency determines that notice will impede a criminal investigation and the law enforcement agency has made a request that the notification be delayed. Any delayed notification will be made after the law enforcement agency notifies CHDI that the notification will not compromise the criminal investigation. If notice of a Breach of Security is provided to a resident pursuant to this paragraph, then CHDI must notify the Attorney General of the Breach of Security no later than the time when notice is provided to the resident. If notice is given to residents pursuant to this paragraph of a Breach of Security that involves a resident's Social Security Number, then CHDI must offer each affected resident appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twelve (12) months. CHDI shall provide all information necessary for a resident to enroll in the services and must include information on how the resident can place a credit freeze on the resident's file.

F. State Contracts

The terms of a state contract may have more specific, or different, notification requirements or privacy and security obligations than are set forth in this policy or in CHDI's HIPAA policies and procedures. In the event of actual or suspected breach of Covered Information, the Security Officer shall review applicable state contract(s) to determine whether there are any additional considerations or obligations related to the incident. In the event of a conflict between the terms of the state contract and this policy, the terms of the state contract shall control.

G. Violations

Any individual who is found, after appropriate investigation, to have violated the provisions of this policy will be subject to disciplinary action, up to and including immediate termination.

Nothing in this policy is intended to modify an employee's right to access their own files in accordance with CHDI policy and applicable law.

H. Review

This policy, and the measures used to protect confidential information, shall be reviewed at least annually and updated as deemed reasonable or necessary.

Child Health and Development Institute
Effective Date: July 1, 2014

-REQUIRED-

SUBJECT: Certain Additional Privacy Protections for Protected Health Information Policy

PURPOSE:

The purpose of this policy is to incorporate additional privacy and confidentiality protections for PHI.

POLICY:

It is the policy of the Child Health and Development Institute to protect the privacy and confidentiality of protected health information. Both state and federal laws impose requirements on how protected health information created or maintained by a business associate on behalf of a covered entity may be used and disclosed by the business associate. CHDI, in its capacity as a business associate of the various covered entities with which it works, intends to comply with all applicable laws protecting the privacy and confidentiality of protected health information, including, but not limited to, the applicable Security and Privacy Rules established under HIPAA.

PROCEDURES:

1. **Generally**. The CHDI shall not use or disclose protected health information unless it is permitted or required by the applicable Business Associate Agreement and Connecticut or Federal law. CHDI shall use and disclose protected health information in accordance with the requirements of its Business Associate Agreements with the covered entities with which the CHDI works. The Security Officer shall be consulted when necessary before permitting the use or disclosure of protected health information.
2. **Requirements for Use and Disclosure of Protected Health Information.** CHDI may use and disclose protected health information only if such use or disclosure, respectively, is in compliance with each of the following requirements, each of which shall be documented in the Business Associate Agreement:

a. CHDI may use and disclose protected health information only as permitted and required in accordance with the applicable Business Associate Agreement. CHDI may not use or further disclose the information in a manner that would violate HIPAA, if done by the covered entity, except that the Business Associate Agreement may permit CHDI to use and disclose protected health information for the proper management and administration of CHDI, and to carry out the legal responsibilities of the CHDI, provided that:

i. The disclosure is required by law; or
ii. CHDI obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and the person notifies CHDI of any instances of which it is aware in which the confidentiality of the information has been breached.
iii. The Business Associate Agreement may permit CHDI to provide data aggregation services relating to the health care operations of the covered entity.

b. CHDI will not use or further disclose protected health information other than as permitted or required by the Business Associate Agreement or as required by law;

c. CHDI will use appropriate safeguards to prevent use or disclosure of protected health information other than as provided for by the applicable Business Associate Agreement;

d. CHDI will report to the covered entity any use or disclosure of protected health information not provided for by the applicable Business Associate Agreement of which it becomes aware;

e. CHDI will ensure that any agents, including a subcontractor, that creates, receives, maintains, or transmits PHI on behalf of CHDI, agrees to the same restrictions and conditions that apply to CHDI with respect to such information;

f. CHDI will make available protected health information to an individual who is the subject of such information in accordance with HIPAA requirements;

g. In accordance with the applicable Business Associate Agreement, and as permitted by the HIPAA regulations, CHDI shall provide access, at the request of covered entity, and in the time and manner designated by covered entity, to protected health information in a designated record set,

to covered entity or, as directed by covered entity, to an individual in order to meet the requirements under 45 C.F.R. § 164.524.

h. CHDI will make available protected health information for amendment and incorporate any amendments to protected health information in accordance with HIPAA requirements;

i. CHDI will make available the information required to provide an accounting of disclosures in accordance with HIPAA requirements;

j. To the extent the Corporation is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Corporation shall comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation.

k. CHDI will make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by CHDI on behalf of, the covered entity available to the Secretary of the United States Department of Health and Human Services for purposes of determining the covered entity's compliance with HIPAA; and

l. CHDI will, upon termination of the Business Associate Agreement, if feasible, return or destroy all protected health information received from, or created or received by CHDI on behalf of, the covered entity that CHDI still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the Business Associate Agreement to the protected health information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

m. CHDI will authorize termination of the Business Associate Agreement by the covered entity, if the covered entity determines that CHDI has violated a material term of the contract.

n. The additional privacy protections specified in Sections 3 – 7 below shall also be incorporated into CHDI's Business Associate Agreements with covered entities.

3. **Prohibition on Sale of Electronic Health Records or Protected Health Information.**

a. CHDI will not directly or indirectly receive remuneration in exchange for any protected health information of an individual unless the remuneration meets an exception described in Section 3(b) below or the covered entity has obtained from the individual, in accordance with HIPAA requirements, a valid authorization that includes a specification of

whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual.

b. The foregoing limitation shall not apply when the remuneration is exchanged for protected health information for certain purposes specifically permitted by HIPAA, such as for certain public health activities, research, and treatment, in accordance with HIPAA requirements. In addition, the prohibition does not apply to remuneration that is provided by a covered entity to CHDI for activities involving the exchange of protected health information that CHDI undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement, or to a subcontractor for activities that the subcontractor undertakes on behalf of and at the specific request of the Corporation pursuant to a business associate agreement; to an individual, when such individual requests access or an accounting of disclosures; required by law as permitted under HIPAA; or for any other purpose permitted by HIPAA, where the only remuneration received by the covered entity or the business associate (as applicable) is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law..

c. Any questions a workforce member may have as to whether CHDI may receive remuneration in exchange for any protected health information should be directed to the Security Officer.

4. **Application of Minimum Necessary Standard**.

a. When using, disclosing, or requesting protected health information as permitted or required under a Business Associate Agreement, CHDI shall limit such protected health information, to the extent practicable, to the limited data set, or, if required, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request.. When guidance to be issued by the Secretary as to what constitutes "minimum necessary" becomes effective, CHDI will follow such guidance, as applicable, in using, disclosing, and requesting protected health information.

b. When disclosing protected health information as permitted or required under a Business Associate Agreement, CHDI will determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

c. The minimum necessary requirement does not apply to:

i. Disclosures to or requests by a health care provider for

treatment;

ii. Uses or disclosures made to the individual, as permitted or required under HIPAA;

iii. Uses or disclosures made pursuant to a valid HIPAA authorization;

iv. Disclosures made to the Secretary in accordance with HIPAA requirements;

v. Uses or disclosures that are required by law; and

vi. Uses or disclosures that are required for compliance with HIPAA.

5. **Fundraising and Marketing Communications Involving the Use or Disclosure of Protected Health Information.** CHDI shall use and/or disclose protected health information on behalf of a covered entity in connection with any fundraising or marketing communication for or on behalf of the covered entity only in compliance with all HIPAA requirements, including, as applicable, receipt by the covered entity of a valid authorization from the recipient of any communication for any such purpose.

"Marketing" is defined in the list of key HIPAA definitions attached to these policies. Any question as to whether a communication involves marketing or requires a HIPAA authorization from the Individual who will be receiving the communication should be directed to the Security Officer.

6. **Requested Restrictions on Certain Disclosures of Health Information**.

a. If an individual requests that CHDI restrict the disclosure of the individual's protected health information to carry out treatment, payment, or health care operations, CHDI will comply with the requested restriction if:

i. except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and
ii. the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

b. Any workforce member who receives a request from an individual for a restriction as described in Section 6a. shall notify the Security

Officer, and the Security Officer shall thereafter notify the applicable covered entity.