

CONNECTICUT CHILDREN'S MEDICAL CENTER
[CCMC Organizational Manual]

Title: Social Security Numbers and Personal Information	
Date of Origination: September 2008	Date Last Revised: September 2008
Approved By: Corporate Compliance Committee	Approval Date: October 2008

- I. Policy:** It is the policy of Connecticut Children's Medical Center (Connecticut Children's) to protect the confidentiality of personal information obtained and used in the course of business from employees, patients, families and other clients.
- II. Rationale:** Misuse of Social Security Numbers and personal information by third parties, including but not limited to identity theft, may be detrimental to individuals. To minimize the risk of such activity related to personal information collected during the course of business, processes shall be established to ensure the protection of this information.
- III. Definitions:**
- A. Personal Information - shall mean information capable of being associated with a particular individual through one or more identifiers, including but not limited to, a Social Security Number (SSN), a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number. It 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.
- B. Breach – shall mean unauthorized access to or acquisition of documents, electronic files, media, data or computerized data containing personal information. This includes events when (1) the access to the personal information has been compromised; (2) the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; or (3) the encryption of personal information has been cracked.
- C. Acquisition – shall mean lost or stolen documents containing personal information; loss of server, desktop, laptop, or personal digital assistant (PDA) containing unencrypted personal information.
- IV. Procedure:**
- A. Protecting Personal Information/ Prohibiting Unlawful Disclosure of Personal Information/ Limiting Access to Personal Information
1. Staff shall limit the collection of personal information to that which is necessary for the purposes it has intended. This personal information shall be collected by fair and lawful means.
 2. Staff shall obtain and use personal information only for its intended purpose (except as permitted by law).

3. All documents containing personal information shall be in locked or secured areas.
 4. Computer applications containing personal information shall be maintained on secured, authorized-access computer stations only.
 5. Transmissions of data or documents containing personal information shall be encrypted prior to leaving the Connecticut Children's secured information system.
 6. Vendors shall sign a Connecticut Children's Business Associate Agreement prior to receipt of any documents or data containing personal information.
 7. Documents containing personal information shall be shredded prior to disposal. Pending this shredding, waste documents containing personal information shall be stored in secured bins, in secured areas.
 8. Electronic devices, including but not limited to computer hard drives, shall be destroyed by a certified entity prior to disposal. Such destruction may include: overwrite (per Department of Defense standards), degaussing, physical destruction or a combination of these.
 9. External entities contracted to provide waste document and electronic destruction shall provide Connecticut Children's with certificates of destruction.
- B. Disclosing Breaches of Security of Personal Information
1. Staff shall contact the Director of Compliance or Director of Risk Management in the event of a breach or suspected breach (reasonable belief) of personal information.
 2. The Director of Compliance or Director of Risk Management shall notify the Privacy Officer and Security Manager and initiate an investigation. The investigation shall:
 - a. Determine the nature and scope of the incident;
 - b. Identify the individuals affected;
 - c. Identify and implement corrective action to prevent further breaches; and
 - d. Retrieve the personal information or restore the reasonable integrity of the data system (if applicable).
 3. If the investigation validates that personal information was accessed by an unauthorized person through a breach of security, and the breach may likely result in harm to individuals whose personal information was accessed, and law enforcement has not requested a delay in notification, the Director of Compliance or Director of Risk Management, in collaboration with the applicable Department Leader and General Counsel, shall notify individuals whose personal information was accessed. Notification may be provided by one of the following methods:
 - a. Written notice;
 - b. Telephone notice;
 - c. Electronic notice;
 - d. Substitute notice (if cost of above notices would exceed \$250,000 or more than 500,000 persons are affected). Substitute notice may

include: electronic mail; conspicuous posting; or notification to state-wide media, including newspapers, radio and television.

4. If the investigation determines that the breach was by Connecticut Children's staff and was intentional, notification shall be made to Human Resources. In such circumstances, the involved individual shall be subject to discipline, up to and including termination.

C. Contacting Connecticut Children's

1. Patients, families and other individuals may contact the following individuals if they have questions and/or concerns about personal information and/or this policy:
 - a. Director of Risk Management – (860) 545-9016
 - b. Director of Compliance – (860) 545-8123
 - c. Privacy Officer – (860) 545-8520

V. **References:**

Connecticut General Statute §36a-701b and Public Act 08-167
Patient Health Information Confidentiality Policy
Confidentiality Agreement
Information Security Plan