

HILL HEALTH CORPORATION POLICY AND PROCEDURES

SUBJECT: Privacy Protection Policy for Personal Information held by Hill Health Corporation

PURPOSE: This policy implements the requirements of Public Act 08-167, codified in Connecticut General Statutes section 42-471. The Act requires “any person in possession of personal information of another person [to] safeguard . . . the information from misuse by third parties.” Personal information means “information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a date of birth, 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, and 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.” The Act further requires any person who collects Social Security numbers in the course of business [to] create a privacy protection policy which shall be published or publicly displayed.”

POLICY: It is the policy of Hill Health Corporation to limit the acquisition of personal information to essential business purposes and to protect the confidentiality of personal information it obtains from its employees, contractors, patients, and other persons and uses in the course of its business. This policy supplements existing Hill Health Corporation policies that address security in employees’ use of the Internet and email and policies that address privacy and security of protected health information and other personal information contained in patients’ (including employee-patients) health records.

PROCEDURES:

1. Acquisition of personal information. Personal information is obtained from employees, volunteers and some contractors in the course of conducting Hill Health Corporation business. It is used predominantly by the Human Resources Department as a necessary tool in the course of personnel-related activities (hiring, background checks, credentialing), by the Patient Accounts Department for contracting and credentialing providers with insurance companies, and by the Business Office in payroll, pension and related activities. Supervisors and managers may have copies or excerpts from employee records that contain personal information. Personal information will only be requested when it is essential for carrying out Hill Health Corporation business.
2. Maintenance and storage of records containing personal information. Paper copies of records containing personal information or records stored on electronic media will be stored in locked cabinets or in locked offices or areas. Computer records containing personal information, whether on a network or a work station or laptop hard drive, will be password protected and accessible only to authorized Hill Health Corporation employees or agents.
3. Access to records containing personal information. Records containing personal information, whether paper or electronic, may be accessed only by authorized Hill Health Corporation employees having a legitimate business need to have access to those records. Authorization may be granted only by the Director of Human Resources, the Controller and the Director of Management Information Systems/Security Officer to employees who are trustworthy and who have passed background checks. Employees granted access must take all necessary precautions to ensure the security of records in their possession or control. Supervisors may not maintain separate employee records that contain personal information except to the extent they are essential for legitimate Hill

Health Corporation business.

4. Disclosing or transmitting records containing personal information. Records containing personal information will be disclosed or transmitted only to persons or entities having a legitimate business need for the record. Records containing personal information will be redacted in part, e.g., using only the last four digits of a Social Security number, when the entire number is not essential for the purpose of the transmission. For records containing personal information that are electronically transmitted to a third party, Hill Health Corporation will employ reasonable and appropriate integrity controls. HIPAA Security Policy # SEC149, entitled "Data that is being transmitted over a communications network," describes some of those controls. Hill Health Corporation will assure that recipients of records containing personal information have an equally protective policy.
5. Destruction of records containing personal information. When records containing personal information are released for disposal under applicable records retention policies, physical records will be destroyed by shredding, and electronic records will be erased or made unreadable or the media on which they are stored will be physically destroyed.
6. Training. The Director of Human Resources, the Director of Health Information Management/Privacy Officer and the Controller, as appropriate, are jointly responsible for assuring that personnel who are subject to this policy are informed of the policy's requirements, how to recognize and avoid a security breach and what actions to take if one occurs. This supplements the MIS Security Policy #SEC200 concerning Internet and email use, which is provided to all new employees at orientation.
7. Violation of the policy. If personal information is disclosed to third parties, i.e., unauthorized persons who are not Hill Health Corporation employees or agents, in violation of this policy, whether intentionally or unintentionally, Hill Health Corporation will, upon discovery of such disclosure:
 - (a) immediately notify the individual whose information was disclosed;
 - (b) provide that individual with all relevant information concerning the disclosure;
 - (c) notify the third party and take further actions that may be appropriate to destroy the record containing personal information or prevent further disclosure;
 - (d) take actions necessary to prevent future disclosures.

Any employee who violates the provisions of this policy will be subject to disciplinary action, up to and including immediate termination. Any contractor who is found to have violated the provisions of this policy will be subject to termination or non-renewal of their contract to the extent permitted by the contract.

DISTRIBUTION: This policy will be posted on the Hill Health Corporation website and in the Outlook public folders.

RESPONSIBILITY: Jointly among the Director of Human Resources, Director of Management Information Systems/Security Officer and Controller.

APPROVED BY THE BOARD OF DIRECTORS: November 19, 2008

REVISED: May 12, 2009 by adding reference to Connecticut General Statutes