



SUBJECT: Privacy Protection Policy

Last Revised Date:

Last Reviewed Date:

PURPOSE: To protect the confidentiality of personal information of employees, patients and other clients of Saint Mary's Hospital (SMH) in accordance with state and federal law.

DEFINITION: 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 driver's license number, a state identification card number, an account number, a credit or debit card 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.

POLICY: It is the policy of the SMH to protect the confidentiality of Personal Information obtained and used in the course of business from its employees and patients.

- PROCEDURE:**
1. Use of Personal Information: Personal Information is only used to conduct SMH business in accordance with state and federal law.
 2. Storage of and Access to Personal Information:
 - Storage: All documents containing Personal Information shall be stored in locked or secured areas. All computer applications containing Social Security numbers shall be maintained on secured servers located in a secured data center.
 - Access: Only persons who have a legitimate business reason will have access to Social Security numbers; such access will be granted through department heads responsible for their job functions. An annual review of minimum necessary access shall be completed by department heads in an attempt to limit access to personal information. Employees granted access to personal information shall protect the confidentiality of this information.
 3. Destruction of Personal Information: Records that include Personal Information, including Social Security numbers, will be maintained in accordance with federal and state laws. When such documents are released for destruction, the physical records will be destroyed by shredding. Hard drives containing electronic records shall be certified by the vendor as destroyed. Back up tapes shall be erased or the data made unreadable prior to destruction.
 4. 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.

Creation Date: September 30, 2008

Key Content Expert: Institutional Privacy/Security Oversight Committee

References: Connecticut Public Act 08-167

JCAHO Reference: