POLICY NAME**: PRIVACY AND SECURITY VIOLATIONS**

POLICY #: 293

DATE ADOPTED: 7/11

REVISION DATE(S):

PURPOSE

To ensure the confidentiality of patient, employee and hospital-proprietary Information in accordance with applicable law and organizational ethics

POLICY

It is the policy of St. Joseph Medical Center to ensure compliance with all applicable state and federal laws providing for the privacy and security of protected health information ("PHI") and electronic protected health information ("ePHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), and confidential information in any form, including electronic, paper and verbal communication. SJMC will investigate alleged violations of confidentiality, privacy or security laws, policies, regulations, standards or procedures. SJMC will impose corrective action on the employee who fails to comply with state and federal laws or with organizational policies, standards or procedures relating to the privacy and security of confidential information. The corrective action will follow the corrective action provisions and guidelines set forth in this policy.

DEFINITIONS

A. Confidential Information means any information, regardless of format, about patients, employees, students, residents, or business operations that is not available to the public. Confidential Information includes, but is not limited to, protected health information, electronic protected health information, employee information, financial and business information, and any other information that is intended for internal use only.

B. employee(s) under this policy means full-time employees, part-time employees, temporary employees, contracted employees, managers, supervisors, volunteers, trainees, and all other persons whose work performance on behalf of the organization is under the direct control of SJMC, whether or not they are paid by SJMC. Employed physicians are considered employees for purpose of this policy.

C. Manager under this policy means an employee who has been assigned responsibility to direct and control employees' job related activities.

D. Protected Health Information ("PHI") is any individually identifiable health information, including demographic information, that is created or received by a SJMC and relates to:

1. The past, present, or future physical or mental health or condition of an individual;

2. The provision of health care to an individual; or

3. The past, present, or future payment for the provision of health care to an individual; and,

4. Identifies the individual, or for which there is a reasonable basis to believe the information can be used to identify the individual.

5. PHI includes information concerning persons living or deceased and may be written, verbal, or in electronic format. The identifiers defined under HIPAA as protected health information are found in the CHI and/or SJMC's policy on De-identification of Protected Health Information rather than in this appendix.

E. Electronic Protected Health Information ("ePHI") is protected health information that is transmitted by or maintained in electronic format.

I. PROCEDURE

A. Levels of Violations

The level of violation is determined according to the severity of the action, whether the violation was intentional or unintentional, the impact on the organization, the impact on a patient or other employee and whether the violation indicates a pattern or practice of improper use or disclosure of PHI, ePHI or other confidential information by the employee. Corrective action will be applied based on the level of violation in conjunction as described herein and consistent with Corrective Action Policy #160.

There are three levels of privacy or security violations:

1. **Type One – Unintentional Violation or Carelessness.** A Type One violation occurs when an employee unintentionally or carelessly accesses, reviews or discloses confidential information to anyone without a legitimate need to know the information to perform job duties. Examples of Type One violations include, but are not limited to:

   a. Inadvertently e-mailing, faxing, mailing, or distributing PHI or other confidential information to the wrong person;

   b. Failing to secure e-mail or other electronic transmission or storage of PHI;

c. Discussion of patient information in a public area without taking reasonable measures to protect the discussion;

d. Not properly verifying the identity and access rights of a person requesting PHI, whether the person is requesting in person, in writing, or by phone;

e. Failure to protect the privacy and confidentiality of medical records or other PHI or ePHI (e.g., permitting improper access or conducting improper distribution or disposal of PHI);

f. Failing to lock computer screen when workstation is left unattended. or failure to appropriately log off the organization's information system;

g. Failure to correctly shut down laptop, with the result that encryption is not enabled;

h. Leaving more than the minimum required PHI on patient's answering machine; or

i. Careless handling of usernames and passwords (e.g., leaving notes with passwords written on them on or near a computer or door key pad).

A Type One violation may be treated as a Type Two or Type Three violation, depending on the magnitude of risk created, prior violations, or other corrective actions imposed on an employee consistent with Corrective Action Policy #160.

2. **Type Two – Intentional Violation or Curiosity/Concern**. A Type Two violation occurs when an employee intentionally accesses, reviews and/or discloses confidential information in an unauthorized manner or for unauthorized purposes, but for reasons unrelated to personal gain. Examples of Type Two violations include, but are not limited to:

   a. Looking up personal information (e.g., birth dates or addresses) of friends or relatives;

   b. Sharing a computer password with another person or group;

   c. Failure to follow device and media control standards, including connecting unapproved devices (e.g. jump drives, flash drives, smart phones, PDAs) to the organization's network;

   d. Accessing and reviewing a patient's record, including an employee's own record or a family member's record, when there is no job-related need to access;

   e. Sharing patient or employee information with any individual who does not have a legitimate need to know the information to perform job duties;

   f. Misuse of information systems; or

   g. Repeated incidents of Type One violations.

A Type Two violation may be treated as Type Three violation, depending on the magnitude of risk created, prior violations, or corrective action imposed on an employee consistent with Corrective Action Policy #160.

3. **Type Three – Violation for Personal Gain or Malice.** A Type Three violation occurs when an employee accesses, reviews, and/or discloses confidential information for personal or monetary gain or with malice. Personal gain or malice includes intentional wrongful actions without justification. Unless extenuating circumstances can be identified, Type Three violations will be treated as a cause for termination under this Policy. Examples of Type Three violations include, but are not limited to:

   a. Inappropriate use or selling of confidential information;
   b. Falsifying or altering patient information;
   c. Obtaining PHI under false representation;
   d. Using confidential information to harass or intimidate other individuals or cause an individual harm, either internal or external to the organization;
   e. Deliberately compromising electronic information security measures;
   f. Gross negligence in handling confidential information;
   g. Subverting network controls or escalating privileges without authorization to do so; and/or
   h. Repeated Type One or Type Two violations.

B. Reporting and Investigation

An alleged violation related to PHI or ePHI require simultaneous reporting to the HIPAA Privacy Official or designee, and to Human Resources.

1. Investigations that involve PHI must be supervised by the Privacy Official. The Privacy Official and the HR Rep will determine who will be involved and the responsibilities of those involved with investigating an alleged violation. The investigation may include, but is not limited to, interviewing the employee involved in the violation, interviewing witnesses, analyzing computer drives and data, reviewing audit logs of system user activity, and any other appropriate actions deemed necessary to determine the relevant facts.
2. SJMC promotes an environment that encourages employees to seek clarification of issues and to report questions and concerns to their immediate supervisor or to utilize the appropriate hotline telephone number. Employees are responsible for reporting

possible violations of standards, guidelines, or policies and will be protected from retaliation by management and other employees, or agents, for their good faith report, complaint, or inquiry. A person who retaliates against an employee making a good-faith report is subject to discipline, up to and including dismissal from employment, or termination of a business relationship with the organization. The non-retaliation policy does not protect an employee from the employee's own actions that violate standards, guidelines, or policies, or applicable laws and regulations.

3. The organization will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an employee who:

    a. Exercises his/her rights or participates in the organizational complaint process;

    b. Files a complaint with the Secretary of Health and Human Services;

    c. Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing; or opposes any act or practice unlawful under state and federal regulations, providing that the individual acted in good faith believing that the practice was unlawful, the manner of opposition was reasonable, and did not involve disclosure of PHI in violation of regulations.

C. Corrective action that results from a violation will be administered in a timely fashion.

1. When user activity audit reports are required, the HR Rep will work with the applicable security designee and others deemed responsible for generating audit reports. Audit reports created as part of investigations are restricted to those with a need to know the information to perform job duties.

2. The HR Rep will be responsible for maintaining investigatory notes and documentation of the investigation and conclusion. HIPAA Privacy Officials and HIPAA Security Officials are required to maintain documentation in the Ethics Point reporting database.

D. Corrective Action

1. Upon conclusion of an investigation, the HR Rep will determine whether an employee's behavior amounted to a Type One, Type Two, or Type Three violation. The HR Rep's conclusion will be reviewed and validated by the Privacy Official and the respective manager of the employee who committed the violation.

2. The general guidelines are:

    a. Type Three violations generally will result in terminating the employee.

b. Type Two violations generally will result in the employee being subject to suspension, Final Warning in lieu of Suspension or termination.

c. Type One violations will be grounds for progressive corrective action and generally will result in the employee receiving a written warning.

3. The HR Rep will review the employee's record for previous corrective action for any policy infraction. Prior acts will be considered in applying the appropriate level of corrective action, consistent with progressive steps described under Corrective Action Policy #160.

II. RESPONSIBILITIES

Supervisor

1. The supervisor is responsible for ensuring that employees receive training on HIPAA, confidentiality, privacy and security practices.

2. The supervisor is responsible for monitoring the activities of his/her staff to ensure that the employee complies with state and federal laws and with CHI and SJMC policies, standards, and procedures.

3. The supervisor is responsible for administering this policy.

4. The supervisor is responsible for reporting violations in accordance with this policy, participating in the investigative processes, and issuing corrective action, as applicable.

Employee

1. The employee is responsible for protecting confidential information, including patient, employee, financial or business-related information, PHI and ePHI, regardless of its location or form, as part of their daily job duties.

2. The employee is responsible for following all applicable state and federal laws, and policies, standards, and procedures as they pertain to confidential information.

3. The employee is responsible for monitoring privacy and security activities that pertain to his/her job.

4. The employee is responsible for promptly reporting any potential violation of privacy or security requirements to his/her supervisor or to an HR Rep. The Privacy Official must

be notified regarding all potential violations of privacy or security of patient information, as set forth in the HIPAA breach notification policy.

5. The employee who does not report a suspected or known violation or makes a report in bad faith or for malicious reasons will receive appropriate corrective action for his/her acts or omissions.

HR Rep

1. The HR Rep, in cooperation with the HIPAA Privacy and/or Security Official, is responsible for conducting a thorough investigation of potential and reported violations.

2. The HR Rep, in cooperation with the HIPAA Privacy and/or Security Official, is responsible for recommending level of violation and level of corrective action in a manner that ensures the consistent application of this Policy.

3. The HR Department will maintain the employee HR record.

4. The HR Rep will ensure that reporting employee professional actions to the appropriate state agency or state board will be carried out by the appropriate professional designee required to make such report (e.g., the organization's risk manager or chief nursing officer).

HIPAA Privacy Official

1. The HIPAA Privacy Official participates in investigations as requested by HR or HIPAA Privacy Officials or their designee and may be required to conduct investigations and determine appropriate corrective actions in cooperation with HR.

2. The HIPAA Privacy Official is responsible for record keeping and required reporting to government entities.

3. HIPAA Privacy Official is required to enter violations into the CHI Ethics Point database and to follow the Breach Notification Policy to determine if notice is required to be provided to a patient and the Department of Health and Human Services.

4. The HIPAA Privacy Official supervises investigations that involve PHI in any form.

REQUIRED REVIEW:	Human Resources; Compliance
POLICY REPLACES:	
DOCUMENTATION:	
REFERENCE:	HIPAA Regulations; Corrective Action Policy #160