



SAMARITAN HEALTH SERVICES
MANUAL OF ADMINISTRATIVE POLICIES

CONFIDENTIAL AND PROPRIETARY INFORMATION

APPROVED: Larry A. Mullins

DATE SIGNED: April 6, 2009

PURPOSE

To establish a mechanism to address confidentiality, security, and the safeguarding of information for Samaritan Health Services (SHS).

POLICY

All information concerning patients, physicians, employees, volunteers, financial data, and business records is confidential/proprietary. All employees and students of SHS will conform to this rule of confidentiality and information will not be released without appropriate authorization.

1. Confidential and proprietary information may not be released without appropriate authorization. Any disclosure of nonwork-related patient information will be considered a breach of confidentiality. Discussions regarding confidential information shall take place in an appropriate setting to minimize disclosure to inappropriate individuals.
2. Employees and students are responsible for safeguarding patient and hospital information against loss, destruction, tampering, and unauthorized copying, access, or use.
3. Confidential trash is defined as any material that contains financial, administrative, and/or clinical results that can be associated with the name of a patient, employee, student, volunteer, or physician. Confidential trash will be disposed of through established confidential trash systems within each department.
4. Only authorized users will be allowed access to computer systems or networks. The security and integrity of computerized information are the responsibility of each system user.
5. Failure to adhere to policies on confidential information and protection of patient privacy may result in corrective action as referenced in the Personnel Policy & Procedures.

PROCEDURE

1. Appropriate confidentiality statements will be signed by each employee or student at the time of hire or placement
 - a. All employees will sign a Code of conduct Statement and an Employee Confidentiality Statement. These statements will be signed at the time of orientation and retained in the employee personnel files in Human Resources. Compliance will be assessed at the time of performance appraisals.
 - b. Volunteers will sign Volunteer Confidentiality Statements when they begin volunteer work. These statements will be retained in the volunteer personnel files in the Volunteer Services office.

- c. Clinical affiliation agreements with colleges and universities will include reference to student responsibilities regarding confidentiality of information and protection of patient privacy. Copies of these agreements will be maintained in the Office of Medical Education
2. Appropriate hospital and department policies and procedures will be reviewed during orientation.
 - a. New employees and students will review pertinent policies on management of information, confidentiality, and patient privacy as part of department orientation.
 - b. Volunteers will receive instruction regarding patient rights and confidentiality.
3. Computer system and network access will be approved by the department manager and the Information Systems Department.
4. Termination of privileges: Upon termination of employment or transfer to another job classification, the following security issues will be addressed by the transferring/terminating manager:
 - a. Notify Information Systems to delete access to hospital networks.
 - b. Access/passwords to department computers/network will be removed.
 - c. Department equipment/property in possession of employee will be returned.
5. As appropriate a department may develop policies, procedures, and guidelines that address department-specific issues related to types of information used in the department and access/restriction by information type and job responsibility. Department policies and procedures may include reference to the following:
 - a. Patient information (medical records needed for patient care, medical information provided to other organizations for continuing care, insurance and/or billing information, data for research purposes.)
 - b. Physician information.
 - c. Hospital information (hospital statistics, quality improvement data, state and federal reporting data, financial information).
 - d. Physical security measures (times when departments, offices, or equipment should be locked, combination-locked doors, computer passwords, security software, alarms).
 - e. Computer systems and network access and back-up procedures. Procedures for recovery of critical information will be included in department disaster plans.
 - f. Disposal of confidential trash (information considered confidential and location of appropriate disposal containers).
6. Confidential trash will be collected and submitted to an authorized firm for final disposal.
7. Appropriate authorization will be obtained prior to release of confidential or proprietary information.

SUBMITTED BY: Human Resources
EFFECTIVE: 2/98
REVIEWED: 2/00
REVISED: 4/09