

SUBJECT: INFORMATION MANAGEMENT PLAN	REFERENCE #1002
DEPARTMENT: HOSPITALWIDE	PAGE: 1
	OF: 19
APPROVED BY:	EFFECTIVE:
	REVISED:

PURPOSE:

It is recognized by _____ Hospital that the provision of healthcare is a complex endeavor that is highly dependent on information. This includes information regarding the individual patient, the care provided, the outcomes of care and the performance of the organization. Due to the collaborative nature of the provision of care, all activities performed are coordinated and integrated throughout all departments and services. It is because of this dependent relationship that information is an important resource that is to be used effectively and efficiently managed. In keeping with the mission statement of _____ Hospital, it is felt that information management is a key component in providing high quality patient care.

GOAL:

To obtain, manage and use information to enhance and improve individual and organizational performance in patient care, governance, management and support processes.

SCOPE AND DIRECTION:

- _____ Hospital is a _____ bed general medical surgical hospital. In addition to the customary complex of emergency, surgical, general medicine, nursing and ancillary services, _____ Hospital provides _____ services to the pediatric through geriatric population. (Include any other patient population specifics here.) Human, hardware and software resources are utilized to supply information to support the organization's information management requirements. To meet these requirements, the Health Information Management, Information Management Systems and hospital administration have paramount shared responsibility for the overall management of information.
- There are organized Health Information Management and Information Management Systems with financial resources allocated by the Governing Body to provide for optimal departmental operations. As the information management environment is constantly changing and becoming more sophisticated, all additional needs for information management, as well as for patient safety considerations related to evolving information management, are assessed with appropriate financial considerations granted through the Governing Body.

MISSION:

The _____ Hospital's Information Systems Department is committed to excellence and leadership, and to providing its users with accurate and useful information in a format which will assist in the performance of job functions.

SUBJECT: DATA CENTER PROTECTION/ EMERGENCY/RECOVERY PLAN	REFERENCE #1102
DEPARTMENT: INFORMATION SYSTEMS	PAGE: 1 OF: 6
APPROVED BY:	EFFECTIVE: REVISED:

POLICY:

- _____ Hospital shall protect the electronic data media source and equipment from damage or loss.
- The Data Center Protection/Emergency/Recovery Plan shall be tested every _____. Deficiencies shall be identified and procedures revised as appropriate.

PROCEDURES FOR REDUCING RISKS:

- Preventive Maintenance of Hardware will be Performed on the Following:
 - Central Processing Unit and Drives:
 - Quarterly by: _____ (name of company)
 - Peripheral Hardware:
 - Bimonthly by Information Systems personnel or on an “as needed basis”
- Protection of Computer Data will be Performed by "Back-up" Storage of Information:
 - Back-up Policy:
 - Entire system will be copied onto magnetic tapes, CDs and/or jump drives each evening as part of the nightly system shutdown procedure. There are no exceptions to this policy.
 - Back-up Storage Policy:
 - Tape Rotation and Storage:
 - ◆ Nightly back-up tapes are to be rotated on a daily basis, seven (7) days per week, 365 days per year.
 - ◆ All back-up tapes are stored off site located _____.
 - Back-up server is located _____.
 - A back-up file shall be tested at least annually to ensure that it can be re-installed.

SUBJECT: DISCLOSURE OF PROTECTED HEALTH INFORMATION DURING DISASTER RELIEF EFFORTS	REFERENCE #2010
	PAGE: 1
DEPARTMENT: HEALTH INFORMATION MANAGEMENT	OF: 2
	EFFECTIVE:
APPROVED BY:	REVISED:

POLICY:

- Providers and healthcare plans covered by the HIPAA Privacy Rule may share patient protected health information to assist in disaster relief efforts and to assist patients in receiving the care they need. Information relevant to the following areas may be shared:
 - Treatment
 - Notification
 - Imminent danger
 - Hospital directory

PROCEDURE:

- Treatment:
 - Healthcare providers may share patient protected health information as necessary to provide treatment.
 - Treatment includes:
 - ◆ Sharing information with other providers (including hospitals and clinics)
 - ◆ Referring patients for treatment (including linking patients with available providers in areas where the patients have relocated)
 - ◆ Coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate healthcare services)
 - Providers may share patient protected health information to the extent necessary to seek payment for these healthcare services.

SUBJECT: HEALTH DATA INTEGRITY	REFERENCE #2102
DEPARTMENT: HOSPITALWIDE	PAGE: 1
	OF: 4
APPROVED BY:	EFFECTIVE:
	REVISED:

POLICY:

_____ Hospital shall protect the privacy of individual identifiable health information. Believing that confidentiality is essential in developing the trust between patients and their providers of healthcare, we are committed to ensuring that patient medical information be disclosed only with informed consent or by statute.

PROCEDURE:

- The Information Management Committee is responsible for the development of organizational standards, policies and procedures concerning timeliness, accuracy, security, privacy and confidentiality, access, integrity and uniformity of data of both paper and electronic records consistent with law or regulation.
- Security/Confidentiality of Information:
 - To provide a balance between data sharing and data confidentiality, individuals/ departments have been identified with specific policies/procedures outlining the access to, and need for, data and information.
 - Health Information Management Department personnel will have access to all documentation present in the medical record in accordance with Information Management Committee approved policies and procedures.
 - Nursing personnel will have access to all pertinent patient information to allow for optimum assessment, treatment and care of the patient in accordance with general nursing policies and procedures.
 - Medical staff will have access to all pertinent patient information that will allow them to render optimum treatment to any patient for whom they are the attending, covering or consulting physician in accordance with the medical staff bylaws.
 - Clerical personnel will have access to all necessary patient information that allows for appropriate billing, insurance and financial procedures.
 - The Health Information Management Department will have access to patient information for reporting purposes in accordance with departmental policies and procedures.
 - All other individuals, including ancillary personnel and administrative personnel, will have access to patient data and information on an “as needed” basis, restricted to level of authority, in accordance with hospitalwide policies and procedures governing information security and confidentiality.

SUBJECT: ADMINISTRATIVE SAFEGUARDS - WORKFORCE CLEARANCE AND ACCESS AUTHORIZATION	REFERENCE #2114
	PAGE: 1
DEPARTMENT: HOSPITALWIDE	OF: 2
	EFFECTIVE:
APPROVED BY:	REVISED:

POLICY:

- _____ Hospital shall determine the access of electronic protected health information to employees is appropriate.
- Once degree of access has been established, the employee is issued a log-in and passcode to use when accessing the medical record by the Information Systems Department. The Information Systems Department controls the degree of access of computerized medical records by electronically granting privileges to portions of the record and subsequent database.

PROCEDURE:

- All individuals expected to utilize the _____ Hospital computer system are assigned an access code known only to the members of the Information Systems Department and the employee.
- Employees of the Information Systems Department are prohibited from displaying, accessing or reviewing the employee listing of access codes without authorization or supervision from the Information Systems Department Director, his/her designee, the Privacy/Security Officer or the hospital Chief Executive Officer. Employees of the Information Systems Department are trained in the need to maintain the confidentiality of the access codes information. Any Information Systems Department employee found in violation of this security measure will be placed in the hospital's disciplinary process.
- A master listing of employee access codes is kept in an electronic file in the Information Systems Department. This file is password protected. A backup file is available in the off-site storage facility. The Information Systems Department Director or designee is responsible for updating the employee access codes file on a monthly basis, creating the backup file and storing in the off-site storage facility.
- Prior to assigning employee access codes, each employee attends computer training.