Policy Statement

It shall be the policy of St. Joseph's/Candler Health System, Inc. ("SJ/C") to restrict the access by co-workers, vendors, consultants or individuals to patient identifiable information or Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Purpose

1. To protect the privacy rights of the patient within SJ/C.
2. To comply with the applicable State and Federal regulations.
3. To provide for the protection of patient rights and comply with any applicable regulations.

Entities to Whom This Policy Applies

St. Joseph's/Candler Health System, Inc. ("SJ/C"), applicable physicians and their staff providing services at SJ/C or other affiliates; volunteers at SJ/C; students and faculty participating in educational activities at SJ/C; consultants, contractors and vendors of SJ/C and their personnel.

Definitions

Protected Health Information - individually identifiable health information as defined by federal regulations and transmitted by electronic media; maintained in any medium or transmitted or maintained in any other form or medium. This excludes education records covered by the Family Educational Rights and Privacy Act and employment records.

Individually identifiable health information - information, including demographic data that relates to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,
- And that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

Authorized User - includes co-workers, consultants, contractors, students, physicians and their employees, volunteers and all other persons working on behalf of the System

who have a legitimate need to access computer systems, have executed the System's appropriate confidentiality agreement, and where applicable, a Business Associate Agreement, have been trained on the computer systems for which access is being provided.

Procedure

A. **Access to the Complete Medical Record:** In the following circumstances, individuals may have access to the entire medical record for treatment or health care operation purposes;

1. Healthcare provider for treatment purposes;
2. Appropriate healthcare operations as defined by HIPAA;
3. Individual who is the subject of the information;
4. Any individual directly authorized by the patient (individual who is the subject of the information).
5. Information is required under a privacy rule for enforcement purposes;
6. Use and disclosures that are required by applicable State or Federal laws and regulations.

B. **Disclosure of the Complete Medical Record:** The disclosure of a patient's complete medical record is restricted to only the above referenced purposes.

C. Co-worker or Authorized User Access

Authorized users of the software systems, including but not limited to Meditech, within SJ/C shall be restricted to the access necessary for those individuals or classes of individuals to carry out their job duties. The categories of Protected Health Information needed to successfully perform their job obligations shall be defined by the job description associated with their position. The individual's access shall be defined and restricted as follows:

1. The applicable job code shall have restrictions to the software systems;
2. Each individual's job description or contract shall define the individual's access to the software systems and Protected Health Information;
3. The Information Systems Department shall maintain job codes as they correlate with the job descriptions.

D. **Enforcement**

1. Authorized Users shall be trained in the appropriate software systems for which the information for their job and job functions are maintained;
2. Authorized Users shall be reviewed periodically as to the appropriate computer access necessary to perform their job.
3. Each Authorized User shall be bound by the confidentiality provisions and policies of SJ/C, as well as the applicable State and Federal regulations.
4. Each Authorized User shall also execute a confidentiality agreement, and where applicable, a Business Associate Agreement, prior to obtaining access to the Protected Health Information maintained at SJ/C.

E. **Compliance**

1. Each Authorized User who obtains or accesses Protected Health Information within SJ/C shall comply with all applicable policies and procedures.
2. In the event that a co-worker or unauthorized user violates the access granted for their job description shall be subject to disciplinary action – up to and including termination.
3. Other individuals (not co-workers), whether authorized or not, who inappropriately access or use Protected Health Information within SJ/C will be subject to legal actions and may have their access permanently removed.

Approved:

_____

Signature

Original Implementation Date: 04/09/2003
Effective System Date: 06/18/2015
Next Review Date: 06/2018
Originating Department/Committee: HIM/Legal Services Dept.
Reviewed: 8/11/2006; 06/2009; 06/2012, 06/2015
Revised: 8/17//2006, 06/2009, 06/2012
Rescinded:
Former Policy Number(s):
Legal Reference: The Health Insurance Portability and Accountability Act of 1996
Cross Reference: Administrative Policy #1081-A Confidentiality of Patient and Business Information
Administrative Policy #1166-A Disclosing PHI for Research Release
Administrative Policy #1171-A– Faxing Protected Health Information