Policy Statement

It will be the policy of St. Joseph's/Candler Health System (SJ/C) to protect the confidentiality of patient records, quality assessment data obtained from patient records, peer review information, medical review information, and SJ/C business and other information obtained by SJ/C co-workers, agents and others providing services in or to SJ/C in the course of their relationship with SJ/C. This policy provides terms and conditions regarding unauthorized use, dissemination or communication of Confidential Information and provides guidance in the use of camera phones.

Definition of Terms

Confidential Information - For purposes of this policy, confidential information includes both patients' Protected Health Information, as well as proprietary Business Information as defined below. The information is obtained during the individual's course of employment or contractual service to the organization – regardless of the type of media used (i.e., paper, computerized, verbal).

Protected Health Information (PHI) - 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 is 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

Business Information: Includes all information, correspondence, data, and materials, whether given verbally, stored on paper, computer disk, microfilm or any other media, that comes into the knowledge or possession of any individual providing services to the System during such individual's or entity's relationship with SJ/C. This also includes software

applications (including third party software licensed for use by SJ/C); SJ/C financial, personnel, business planning, quality assurance and risk management information.

Breach of Confidentiality – Any unauthorized access, use, unauthorized disclosure, dissemination or communication of Confidential Information (as defined above).

Restricted Areas: Areas within the hospitals and SJ/C entities to which access is limited to specific co-workers, patients or visitors. These areas are identified by appropriate signage. Restricted Areas also includes all areas where Protected Health Information may be posted and areas that may contain sensitive or proprietary business information or equipment.

Procedure

A. All individuals providing services to the System will be required to keep all Confidential Information of which they become aware in connection with their relationship with SJ/C strictly confidential and agree to:

1. NOT copy or disclose it in any way to any third party, including other co-workers or agents of SJ/C,
2. NOT use it in any way except as necessary and authorized pursuant to the policies and procedures of SJ/C;
3. NOT to remove any Confidential Information from the facilities of SJ/C without the prior written consent of SJ/C;
4. keep others from disclosing the Confidential Information; and
5. immediately notify a supervisor or appropriate administrative personnel if the Individual or entity providing services to the System obtains knowledge of any unauthorized access, use or disclosure of Confidential Information.

B. Specific procedures for each type of individual or entity providing services to the System is contained in the Exhibits attached to this policy (Exhibit A is for SJ/C Co-workers; Exhibit B is for individuals providing services to the System, and guests or volunteers of the System (i.e., students). As described in the applicable Exhibits:

- Prior to providing any services at SJ/C, all individuals or entities providing services to the System will be required to sign a Confidentiality Agreement - which will be maintained by the SJ/C Legal Services Department or Human Resources Department, as appropriate.
- Information regarding the requirements of this policy and the other policies referenced in this policy will be presented to and discussed with the individual or entity providing services to the System.
- The individual or entity providing services to the System will be provided a copy of this policy.
- Periodically, all individual or entities providing services to the System will be required to sign a statement regarding confidentiality.

C. Each System contact, as designated on the attached Exhibits, is obligated to ensure

that all applicable individuals reporting to the department understand the Confidentiality Agreement and the policies referenced, and to provide information and an opportunity to ask questions about the policies referenced in this policy and the Confidentiality Agreement.

D. Use of camera phones or cameras – for photography purposes by co-workers, contractors, visitors - is prohibited in all Restricted Areas. Violations of this policy may result in immediate removal of the camera phone and/or the co-worker from the restricted area, and retention of the camera phone for inspection by the company and/or legal authorities. For co-workers, violations of this policy may also result in immediate discipline "including the possibility of termination." Limited exceptions will apply where the co-worker in possession of the camera phone or camera has been provided with advanced written authorization to use it by an authorized member of company management and the camera phone is being used in an authorized manner to further company business.

E. The Information System network servers will be restricted to authorized personnel. Authorized visitors will be supervised.

F. Refer to **Administrative Policy #1162-A Release of Health Information** for specific procedures regarding the release of medical records information.

G. Refer to **Administrative Policy #1034-A News Media Relations/Accredited Spokespersons** for specific procedures regarding release of information to the news media or similar organizations.

H. Refer to **Administrative Policy #1171-A Faxing Protected Information** for procedures regarding transmittal of information by such methods.

I. Refer to **Administrative Policy #1117-A Access to Computer Systems** for procedures regarding security violations.

J. Refer to **Administrative Policy #1108-A Destruction of Patient/Business Information** for procedures regarding destruction of information.

K. Refer to **Administrative Policy #1163-A Confidentiality-Breach Policy** for procedures regarding breaches of patient information or PHI.

Disciplinary Action

A. Any individual or entity who observes or discovers any unauthorized access to or use or disclosure of Confidential Information has the responsibility and requirement to report the incident (or suspected incident) to SJ/C's Privacy Officer, Corporate Compliance Officer, or Hotline at #819-LAWS(5297). Individuals will follow the

procedures outlined in **Administrative Policy #1158-A Corporate Compliance Program** Section C (Reports of Wrongdoing).

B. Any individual or entity who violates the provisions of this policy will be subject to disciplinary actions - up to and including termination.

C. SJ/C may take legal action against an individual or entity for breach of the Confidentiality Agreement, Business Associate Agreement and/or disclosure or use of Confidential Information.

Approved:

Signature

Original Implementation Date: See former policies.
Next Review Date: 04/20/2024
Originating Department/Committee: Legal Services Department
Reviewed: 06/06, 10/08, 02/10, 11/11, 02/15, 01/18, 04/21
Revised: 2/26/02**,** 06/30/05, 10/08, 02/10, 11/11, 04/21
Rescinded:
Former Policy Number(s): **CH – 6002 – Confidentiality of Patient Information**
Original: 8/2/89
Reviewed: 12/94
Revised: 8/95

SJH - 8310-RI-12 – Patient Confidentiality
Original: Unknown
Reviewed: 2/95, 3/98

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

EXHIBIT A

PROCEDURE FOR CO-WORKERS AND INDEPENDENT CONTRACTORS FROM "OUTSOURCED" DEPARTMENTS

Information regarding the requirements of this policy and the other policies referenced in this policy will be presented to individuals providing services to the System during System orientation. For Co-Workers, this policy will be discussed individually by Human Resources.

When the individual **goes** through the Human Resources hiring process:

- Human Resources will be responsible for providing the Confidentiality Agreement to the individual and ensuring the agreement is signed prior to the individual providing services to the System.

- Human Resources will maintain the original copies of the Confidentiality Agreements.

Each year, as part of the annual training review requirement, co-workers will be required to sign an acknowledgment of the Confidentiality Agreement – this requirement may take place within the computerized annual training modules.

EXHIBIT B

PROCEDURE FOR INDEPENDENT CONTRACTORS FROM "OUTSOURCED" DEPARTMENTS

When the individual **does not** go through the Human Resources hiring process:

- Prior to providing any services at SJ/C, all individuals providing services to the System shall be required to sign a Confidentiality Agreement.

- The Department responsible for the contractual relationship with the agency or vendor will be responsible for providing the Confidentiality Agreement to the individual and ensuring the agreement is signed prior to the individual providing services to the System. The responsible Department will forward original copies of the confidentiality Agreements to the Legal Services Department.

- Legal Services Department will maintain the original copies of the Confidentiality Agreements.

- Each year, as part of the annual evaluation or within the annual required training (which may take place within the computerized annual training modules), Individuals providing services to the System will be required to sign an acknowledgement of the Confidentiality Agreement.

Information regarding the requirements of this policy and the other referenced policies will be presented to individuals providing services to the System during System orientation – where applicable. This policy will also be discussed with each individual providing services to the System by the Department responsible for contracting with the Agency or Vendor.