TITLE: CONFIDENTIALITY		**DOCUMENT TYPE:** POLICY
ENTITY: CSC	**CITATION:** 45 C.F.R. PARTS 160 AND 164; 42 CFR 482.13(d)	**DEPARTMENT:** ADMINISTRATION
AUTHORED BY: LEGAL AFFAIRS	**RESPONSIBILITY:** PRESIDENT AND CEO	**APPROVED BY:** PRESIDENT AND CEO
REVIEWED: BIANNUALLY	**EFFECTIVE DATE:** 2/10/2017	**PREVIOUS TITLE:** N/A
LAST REVIEWED WITHOUT CHANGES: N/A	**LAST REVISED:** 10/1/2014; 1/16/2009; 3/22/2004	
POLICY MANUAL: ADMINISTRATION		
RELATED POLICIES: CSC HEALTH INFORMATION SECURITY AND PRIVACY PROGRAM		

CONFIDENTIALITY

PURPOSE: To protect the confidentiality and security of records and information of Center for Special Care, Inc. and its affiliates ("CSC").

POLICY: Employees and others that have access to confidential and proprietary information while carrying out their responsibilities at CSC have a duty to protect the confidentiality of such information. This obligation applies to all CSC records and information created or obtained during the normal course of business that is not generally available to the public, as described herein.

The CSC Health Information Security and Privacy Program sets forth specific requirements to protect the privacy and security of individuals' protected health information, in compliance with federal law. Employees and other authorized users with access to CSC records and computer systems are also required to comply with the Health Information Security and Privacy Program and its related policies and procedures.

DEFINITIONS:

"**CSC Confidential Information**" - Information, records and data that are subject to this policy include, but are not limited to:

1. Individually identifiable health information, including, but not limited to, patient medical records, demographic information, medical, personal or financial identifiers, and financial or payment-related information.
2. Research information and processes.
3. Personal information about employees, physicians, nurses, and other caregivers, and other individuals affiliated with CSC.
4. Information and processes related to medical staff credentialing and privileging and peer review.
5. Employment records of others, including but not limited to, competency and performance evaluations, disciplinary actions, and Employee Health records.

6. Information about relationships with payers and other third parties.
7. Business records and proprietary information including, but not limited to, financial records, audit and accounting records, risk management and compliance activities, quality assurance information, operations, policies and procedures, business development and strategic plans, and similar information.
8. Computer software and information technology processes.
9. Products/devices protected by intellectual property or proprietary rights of any party.
10. Fundraising data and individual donor information held by CSC.
11. Data related to community members and non-patient participants of the Aquatic Rehabilitation Center and HSC Community Services programs.
12. Early Learning Center records.

CSC Confidential Information includes information in any format, including, without limitation, computerized records, manually generated records, paper copies, electronic records, digital records, audio or video recordings, and information obtained orally.

"**Confidentiality**" is the act of limiting access to and disclosure of protected information to authorized persons or parties.

"**Security**" is the act of preventing unauthorized access, use, disclosure, modification and destruction of CSC confidential information.

"**Authorized User**" means any individual or entity that is given access to CSC records, data and/or information technology systems that may contain confidential or proprietary information. This includes, but is not limited to, employees, medical staff members, health care professionals, residents, fellows, students, volunteers, governing board members of any CSC affiliate, committee members, and other individuals or entities carrying out authorized functions or responsibilities.

PROCEDURE:

1. Access to CSC Confidential Information is restricted to authorized users on a need-to-know basis, as determined by their job-related or service-related responsibilities and obligations. Business, financial and corporate records may be accessed and used by authorized business, financial, external auditing, and corporate consultants within the scope of their responsibilities.

2. Any third party granted access to CSC confidential information shall be restricted to those records and information necessary for the purpose(s) set forth in the service agreement. Appropriate confidentiality provisions will be set forth in the service agreement. Any third party that will be accessing CSC patient protected health information and meets the definition of a Business

Associate, , as set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules (codified at 45 C.F.R. Parts 160 and 164) must enter into a Business Associate Agreement.

3. It shall be the responsibility of each CSC employee to report any suspected breaches of this policy to CSC management or to the Corporate Director, Health Information Management/ Privacy Officer.

4. It is the responsibility of each CSC employee and authorized user to comply with the Health Information Security and Privacy Program with respect to individually identifiable health information of CSC patients.

5. It is the responsibility of CSC employees and authorized users to take reasonable precautions to protect CSC confidential information from unauthorized access, use, disclosure, modification and destruction. This includes reasonable steps to ensure the physical and technical security of paper records, as well as all types of files and data, electronic mail, and computing devices, portable devices and or remote access to CSC information systems that may be used to access, store or transmit confidential information electronically.

6. Any CSC employee will be subject to disciplinary action, in accordance with applicable employment policies and procedures, up to and including termination, if he or she:
   - 6.1 Accesses or misuses confidential information other than on a need-to-know basis as determined by his/her job-related or service-related responsibilities and obligations;
   - 6.2 Fails to protect the confidentiality or security of CSC confidential information;
   - 6.3 Fails to prevent disclosure of CSC confidential information to any unauthorized third party;
   - 6.4 Fails to report any suspected breaches of this Policy, CSC policies related to information security, or CSC policies governing health information security or privacy;
   - 6.5 Fails to abide by the CSC Health Information Security and Privacy Program or CSC policies and procedures related to confidentiality, privacy or security of electronic protected health information; or
   - 6.6 Shares computer passwords or permits another person to inappropriately access, alter, delete or use confidential information by the use of his/her unique username and/or password or other token or authentication method assigned to the individual.

7. Any authorized third party who violates this policy may be denied continued access to CSC systems, records and information, may be subject to the termination provisions in the service agreement or Business Associate

agreement, and/or may be subject to legal action for breaching the duty of confidentiality, breach of contractual obligations, or breach of any covenants, express or implied, contained in the service agreement, or applicable legal obligations.

8. With specific regard to patient medical records, the medical record is the property of the entity in which it is created and is used by practitioners in the management and evaluation of patient care. It is maintained for the benefit of the patient, the physician and other caregivers, and the operations of CSC entities. Disclosure of medical record information is allowed in accordance with established policies only, and is the responsibility of the Corporate Director, Health Information Management/Privacy Officer.

9. Upon hire, all new employees must sign an Confidentiality Agreement prior to being given access to any CSC records or computer systems. Managers must forward the signed Confidentiality Agreement to Human Resources for retention in the individual's personnel record.
   9.1 An IT User Access Form must be submitted by the person's Manager before any employee or authorized user can be granted privileges to access CSC's information technology resources. Privileges will be granted only as necessary to carry out his/her duties or job responsibilities. (Refer to the User Access to and Control of Information Systems Policy.)

10. In addition to employees, certain other individuals must sign a Confidentiality Agreement prior to being given access to CSC records or systems, including but not limited to the following:
    - Applicants to the Medical Staff for membership or clinical privileges
    - Clergy
    - Consultants and Individual Clinical Contractors
    -
    - Hairdressers and other providers of personal services
    - Residents, Fellows and Medical Students
    - Trainees/Students
    - Volunteers

    Signed Confidentiality Agreements for non-employees will be retained in the Medical Staff credentialing files, or with the department/manager responsible overseeing the functions and activities of such individual, as applicable.

11. This policy is not intended to invalidate confidentiality protections established in law or other applicable CSC policies, including, but not limited to, employment policies, Medical Staff Bylaws or Rules and Regulations, quality improvement procedures, or other policies providing

specific protection of confidential information.