CENTER OF SPECIAL CARE
POLICIES AND PROCEDURES

TITLE: CONFIDENTIALITY OF CSC INFORMATION	**EFFECTIVE/REVISED DATE**: 5/15/2026
LAST REVIEWED WITHOUT CHANGES DATE: N/A	
RESPONSIBLE DEPARTMENT/COMMITTEE: LEGAL AFFAIRS	
APPROVED BY: PRESIDENT & CEO	
CITATION/REFERENCE: 45 C.F.R. PARTS 160 AND 164; 42 CFR 482.13(D); MEDICAID ADDENDUM TO PROVIDER ENROLLMENT AGREEMENT CONCERNING THE ACCEPTANCE, ISSUANCE, AND USE OF ELECTRONIC SIGNATURES	
REPLACES/PREVIOUS TITLE: N/A	

CONFIDENTIALITY OF CSC INFORMATION

PURPOSE: To maintain a policy to protect the confidentiality of all records and information of Center for Special Care, Inc. and its affiliates ("CSC"). The scope of CSC Confidential Information covered by this policy is defined below, and is expansive in that it includes information contained in personnel, operational and other business records in addition to patient information that is covered by HIPAA policies and procedures.

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.

CSC policies set forth specific requirements to protect the privacy and security of individuals' "protected health information," as defined by and in compliance with federal law otherwise known as the Health Insurance Portability and Accountability Act or HIPAA. Employees and other authorized users with access to CSC records and computer systems are required to also comply with those HIPAA policies and procedures.

DEFINITIONS:

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

1. Business records and proprietary information including, but not limited to, financial records, audit and accounting records, risk management, patient safety, quality assurance and compliance activities, information related to hiring decisions, corporate governance, contractual relationships, operations, policies and procedures, business development and strategic plans, and similar information.
2. 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.
3. Clinical Research programs, studies, and information related to such research participants.

4. Personal information about employees, providers, nurses and other clinical staff, volunteers, students, and other individuals affiliated with CSC.
5. Information and processes related to medical staff credentialing and privileging and peer review.
6. Employment records of others, including but not limited to, competency and performance evaluations, performance improvement, disciplinary actions, and Occupational Health records.
7. Information about relationships between HFSC and payers, and CSC relationships and program/planning materials with grant organizations, lessors/lessees, business partners, regulatory agencies, and other third parties.
8. Computer software, systems configuration and information technology processes.
9. Products/devices/data protected by trademark, copyright, or other intellectual property or proprietary rights of any party (including, but not limited to, research partners or vendors providing services/products to CSC).
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 all HSC Community Services sports and residential housing programs.

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

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

"**Security**" is the act of preventing unauthorized access, use, disclosure, modification and/or 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 consultants, or other individuals or entities carrying out authorized functions or responsibilities on behalf of CSC.

PROCEDURE:

1. Access to CSC Confidential Information is restricted to Authorized Users on a need-to-know basis, as determined by their job-related responsibilities and/or other applicable responsibilities and obligations. Business, financial and corporate records may be made available for use by authorized business, financial, external auditing, and corporate consultants within the scope of their work on behalf of CSC.

2. Any third party granted access to CSC Confidential Information shall be restricted to those records and information that are necessary for the purpose(s) set forth in the engagement or 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 set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must enter into a Business Associate Agreement.

3. It shall be the responsibility of each Authorized User 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 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, laptops, iPads and other computing devices, portable devices, web-based portal access to any government agency, payer or other CSC vendor/partner, and/or remote access to CSC information systems that may be used to access, store or transmit Confidential Information electronically.

5. Any CSC employee will be subject to disciplinary action, in accordance with applicable CSC policies and procedures, up to and including termination, if he or she:
    - 5.1 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;
    - 5.2 Fails to protect the confidentiality or security of CSC's confidential information;
    - 5.3 Fails to prevent disclosure of CSC confidential information to any unauthorized third party;
    - 5.4 Fails to report any suspected breaches of this Policy or other applicable CSC policies related to information security or privacy of personal information;
    - 5.5 Fails to abide by CSC HIPAA policies or CSC Information Systems policies and procedures related to confidentiality, privacy or security of CSC systems or electronic information;
    - 5.6 Shares or misuses computer passwords or log-in credentials; or
    - 5.7 Permits another actor to inappropriately access, copy, retain, transmit, 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.

6. Any other (non-employee) Authorized User or 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 a service agreement or Business Associate agreement, and/or may be subject to all available legal remedies for breach of his/her/its duty of confidentiality, contractual obligations, any professional obligations, or other applicable legal obligations.

7. 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 clinicians in the management, provision and evaluation of patient care. It is maintained for the benefit of the patient, the physician and other caregivers, and the operational needs of CSC entities. Disclosure of medical record information is allowed in accordance with established policies only, and any questions related to disclosure of medical records should be referred to the Director, Health Information Management/Privacy Officer.

8. Upon hire, all new employees must sign a Confidentiality Agreement prior to being given access to any CSC records or computer systems, which will be retained in the individual's personnel record.

9. 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 for overseeing the functions and activities of such individual.

10. **Retention**: Signed Confidentiality Agreements will be retained for duration of employment plus 7 years. For non-employees, signed forms are retained until 7 years after the end of the person's affiliation with CSC.

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 or standards providing specific protection of confidential information.