HEALTH CARE SERVICE CORPORATION

CORPORATE POLICY

Title: CONFIDENTIAL INFORMATION	**Policy No.: 5.03**
Owner/ Approval by:	**Vera Malone, VP, Ethics and Compliance**
Date of Last Review:	**November 2017**
Approved by:	**Thomas C. Lubben, SVP, Chief Compliance and Privacy Officer**
Date of Last Review:	**November 2017**
New Policy ☐	
Revised Policy ☑	**Replaces Policy No.:** **Policy Title:**

POLICY:

Employees of the Company and its subsidiaries (full-time, part-time, seasonal and temporary) and contingent workers (staff augmentation/independent contractor) must protect the confidentiality of information that they handle concerning members and clients both inside and outside the Company. Employees and contingent workers will take necessary and reasonable precautions to avoid unauthorized, inadvertent or incidental disclosures of sensitive, confidential or privileged member, provider member, provider, group, employee, broker and proprietary business information, records or documents. This information includes sensitive personal information (SPI), protected health information (PHI) and business confidential information (BCI) as well as other information the Company considers to be confidential. Within the Company, employees and contingent workers will share information only with those employees and contingent workers who have a legitimate business need to know the information to carry out their assigned duties.

RATIONALE:

The Company and its subsidiaries are committed to taking appropriate steps necessary to safeguard the confidentiality of information in its possession and control.

CONSEQUENCE OF VIOLATION:

Any violation of this policy and procedure by an employee or contingent worker may result in appropriate corrective action, up to and including termination of employment or engagement.

SCOPE:

This policy applies to all individuals engaged in any HCSC work as employees (full-time, part-time, temporary or seasonal) and contingent workers (staff augmentation resources / independent contractors). Employees and contingent workers are defined according to the Workforce Classification Policy in the HCSC Workforce & Employment Policies.

DEFINITION:

Sensitive Personal Information (SPI): is an individual's first name or initial and last name, along with any of the following: Social Security Number, driver's license number or government issued ID number, account, credit or debit card number in combination with any required security code, access code or password that would allow access to an individual's financial account. A list of SPI identifiers and categories is provided in the Sensitive Personal Information (SPI) Categories Decision Guidance located on the Decision Guidance page of the Privacy Office intranet site.

Protected Health Information (PHI): is individually identifiable health information that is used, disclosed accessed or maintained by a Covered Entity or its business associate. PHI does not include individually identifiable health information that HCSC may hold about employees in HCSC's capacity as an employer. A list of PHI identifiers and categories is provided in the Protected Health Information (PHI) Category & Identifier Listing located on the Decision Guidance page of the Privacy Office intranet site.

Business Confidential Information (BCI): is non-public data that HCSC treats as confidential or that a reasonable person would consider confidential, regardless of whether such information is maintained in paper or electronic. BCI includes, but is not limited to the following: intellectual property, corporate documents & records, legal documents, sales and marketing strategies, prospects and customer lists. A list of BCI identifiers and Categories is provided in the Business Confidential Information (BCI) Decision Guidance located on the Decision Guidance page of the Privacy Office intranet site.

Minimum Necessary: is a key protection of the HIPAA Privacy Rule and requires covered entities and business associates to take reasonable steps to limit the use, disclosure and requests for PHI to the minimum necessary to accomplish the intended purpose or function.

Inadvertent Disclosure: is a disclosure that occurs due to human or system error and results in an unauthorized disclosure of an individual's PHI released to someone other than an HCSC employee. This disclosure must be reported to your management and disclosure tracking must be done.

Incident Disclosure: is a disclosure that is accidentally made during a permitted disclosure. Incidental disclosures can occur while appropriately doing your job and which may not be reasonably prevented. These disclosures need to be reported to your management so that they can monitor for repeat occurrences, but they do not need to be tracked.

Covered Entity: is a person or organization that is a health care provider that engages in certain reimbursement transactions electronically, a health plan or a health care clearinghouse. A Covered Entity is a person or organization that is directly regulated by the HIPAA Privacy and Security Rule. As a health plan, HCSC is a Covered Entity.

Business Associate: is a person or organization that creates, receives or maintains, or transmits PHI on behalf of a covered entity. A business Associate can be a person or organization who provides legal, actuarial, accounting, consulting, data aggregation, management, administration, accreditation, system/application testing or financial services for a Covered Entity when the Covered Entity gives PHI to that person or organization. A Covered Entity can be a Business Associate of another Covered Entity.

ROLES AND RESPONSIBILITIES:

All employees and contingent workers must protect from unauthorized, inadvertent or incidental disclosure of all SPI, PHI, BCI and other sensitive, confidential, proprietary and privileged information in their possession or control.

Employees and contingent workers will use and disclosure PHI, SPI, BCI and other sensitive, confidential, proprietary and privileged information in their possession or control to other employees and contingent workers only on a “need to know” basis for carrying out their duties while conducting Company business.

Employees and contingent workers will disclose, PHI, SPI, BCI and other confidential, proprietary and privileged information in their possession or control outside the Company only on a “need to know” basis to authorized persons or entities and according to applicable federal and state laws for the purpose of conducting Company business. For additional information refers to Corporate Privacy Policies PO-3 (Safeguarding PHI/SPI/BCI), PO-7 (Minimum Access Protected Health Information) and PO-11 (Request to Access Protected Health Information)

All employees and contingent employees must protect the confidentiality of systems access information including password and security codes. Each employee and contingent worker is responsible for the actions resulting from the use of his or her passwords or allow Employees and contingent workers will not share passwords or allow others to use their computers while logged on.

EMPLOYEE INFORMATION:

During employment or engagement, and contingent workers may become aware of “insider information”. The law prohibits the use of this information for the Company’s, employee’s, contingent worker’s own financial gain. In addition, employees and contingent workers may not “tip” others by sharing this information with them.

Employees and contingent workers will not engage in communications about potential business relationships, purchases, mergers or acquisitions or other organizational changes either internally or with unauthorized third parties except on a “need to know” basis.

Employees and contingent workers are prohibited from appropriating confidential or proprietary Company information for their own personal use.

DISCLOSURE AFTER TERMINATION:

Even after termination of employment or engagement, an employee or contingent workers must take reasonable steps to maintain and protect confidential, proprietary or privileged information

that they received or had access to while engaged as an employee or contingent workers. Failure to do so may result in legal action against the offending party.

PROCESS OVERVIEW:

A formal process must be followed to ensure compliance with this policy on the protection of the Company's confidential, proprietary and privileged information.

PROCESS:

This is the process to comply with this policy.

Description:

Step 1: As part of orientation and on an annual basis thereafter, all employees and contingent workers are required to complete computer based training regarding their obligations to take appropriate steps necessary to safeguard the confidentiality of information in possession and control. This training is assigned by the Ethics and Compliance Department, Privacy Office, Information Security and Government Programs Departments. Employees and contingent workers also receive Divisional Department training as well.

Step 2: All employees and contingent workers are informed of the Code of Ethics and Conduct ("the Code") and this Confidential Information Policy. Employees and contingent workers are also provided an electronic copy of the Code and this policy. All employees are required to sign the Commitment to Ethics Certification at the time of new employee ethics and compliance training and annually thereafter. Employees and contingent workers may sign the required certifications electronically.

Step 3: The signed Certification is maintained by the Ethics and Compliance Department.

ADDITIONAL RESOURCES:

Policy Links:

Workforce Classifications Policy
Compliance with the Law, 5.02
Conflict of Interest, 5.04
Fair Competition, 5.05
Non-Retaliation, 5.06
Internal Controls, Corporate Policy, 3.03