HEALTH CARE SERVICE CORPORATION

CORPORATE POLICY

DEPARTMENT: Ethics and Compliance	
POLICY NUMBER: 5.03	**POLICY TITLE:** Confidential Information
EXECUTIVE OWNER: EVP, Chief Administrative Officer & Chief Ethics, Compliance and Privacy Officer	**BUSINESS OWNERS:** Executive Director, Corporate Compliance and Executive Director, Privacy Office
ORIGINAL EFFECTIVE DATE (IF KNOWN): 05/01/2008	**COMMITTEE APPROVAL DATE:** 05/08/2025

I. SCOPE

This policy applies to employees and contingent workers as defined in the HR Workforce Classification Policy ("Workers") of Health Care Service Corporation, a Mutual Legal Reserve Company, as well as its majority-owned (greater than 50%) subsidiaries (collectively "HCSC").

II. PURPOSE

HCSC is committed to protecting and safeguarding Confidential Information in its possession and control. Therefore, the purpose of this policy is to establish the guidelines regarding the use, access and disclosure of Confidential Information as defined herein.

III. POLICY

A. CONFIDENTIAL INFORMATION DEFINED

Confidential Information at HCSC includes Personally Identifiable Information (PII) and Business Confidential Information (BCI) and applies to information HCSC maintains about a member, Worker, customer, broker, provider and its business operations and is defined as the following:

1. **Personally Identifiable Information (PII)** - PII is any data that uniquely identifies an individual. The definition of PII varies in federal and state laws, as well as HCSC government and customer contracts. HCSC's definition of PII includes; Protected Health Information (PHI), State Personal Information (SPI) and Contract Personal Information (CPI) and can be delivered in paper, oral or electronic form.

    a. **Protected Health Information (PHI)** - PHI is individually identifiable health information that is created, received, accessed, used or maintained by a Covered Entity or a Business Associate and relates to:

i. An individual's past, present or future physical or mental health condition;
ii. The payment or provision of health or dental services; and
iii. The 18 specific identifiers listed in the Protected Health Information (PHI) section of the PII & BCI Definitions and Data Elements Decision Guidance.

Note: PHI does not apply to individually identifiable health information HCSC may hold about Workers in its capacity of employer.

b. State Personal Information (SPI) - SPI is defined under certain state laws as an individual's first name or initial and last name, along with:
i. 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; and
ii. Biometric Data; and
iii. Other personal identifiers (i.e., PHI data elements) as defined in specific state law.

c. Contract Personal Information (CPI) - CPI includes data elements that may be included in certain HCSC government and customer contracts. For example:
i. Qualified Health Plan identifier
ii. Net premium amount
iii. Household income
iv. Advance Premium Tax Credits
v. Applicant Cost Sharing Reduction, etc.

2. Business Confidential Information (**BCI)** - BCI includes any company trade secrets, proprietary information, and other legally protected information maintained by HCSC which may not be authorized for disclosure to outside third parties or the public. Examples include but are not limited to the following: product pricing, provider and facility discounts, access to company information systems, business strategy, client accounts, source code, financial data, or HCSC contractual agreements.

B. ROLES AND RESPONSIBILITIES

1. Workers are required to protect all Confidential Information to avoid any impermissible, unauthorized, inappropriate or incidental access, release or disclosure of such information either internally or externally.

2. When disclosing Confidential Information internally, Workers must only share the minimum amount of information with Workers who have a legitimate business need to access such information to carry out their assigned job responsibilities.

3. When releasing or disclosing Confidential Information externally, Workers must only disclose the minimum amount of Confidential Information to those individuals or entities that are authorized by HCSC in accordance with all applicable HCSC Procurement, Privacy and Security policies and procedures.

4. In addition, all Workers are required to protect HCSC's information systems containing Confidential Information by appropriately using and managing their passwords and security codes. Workers are responsible for complying with all HCSC Security Policies

including those that specifically prohibit the sharing of passwords and allowing others access to their computers when logged on.

C. ACCESS TO “INSIDER INFORMATION"

1. Workers may become aware of “insider information.” The law prohibits the use of insider information by a Worker for their own financial gain. HCSC also prohibits the sharing of this information with others inside or outside the organization.

2. Workers may not engage in communications about potential business relationships, purchases, mergers or acquisitions, or other organizational changes inside or outside the organization other than on a “need to know” basis and are prohibited from misusing using any Confidential Information for their own personal gain.

D. CONSEQUENCE OF VIOLATION

Any violation of this policy by a Worker may result in corrective action, up to and including termination of the Worker and a termination of the Worker’s engagement with HCSC.

E. DISCLOSURE AFTER TERMINATION

When a Worker’s employment ends, or engagement ends, the Worker agrees to maintain and protect any confidential, proprietary, or privileged information they had access to while engaged as a Worker. Failure for either party to do so may result in formal legal action.

IV. CONTROLS/MONITORING

Control/Monitoring Document or Control/Monitoring Description	Control/Monitoring Owner
As part of orientation, and on an annual basis thereafter, all Workers are required to complete computer-based training regarding their obligations to take appropriate steps necessary to safeguard the confidentiality of information in their possession and/or control. This training is assigned by the Ethics and Compliance Department and combines information from the Ethics and Compliance Department and the Privacy Office. Workers also receive Divisional Department training as well.	Ethics and Compliance
All Workers are informed of the Code of Ethics and Conduct (“the Code”) and this Confidential Information Policy. Workers are provided an electronic copy of the Code which includes a link to this policy. All Workers are required to sign the Commitment to Ethics Certification at the time of New Hire Ethics and Compliance training and annually thereafter. Required certifications are signed electronically. The signed Certification is maintained in HCSC’s Learning Management System.	Ethics and Compliance

V. RELATED DOCUMENTS

1. HCSC Corporate Policy Manual
2. Compliance Program Charter
3. Corporate Policy 5.01 - Compliance Program
4. Corporate Policy 5.02 - Compliance with the Law
5. Code of Ethics and Conduct
6. Code of Ethics and Conduct for Vendors
7. Code of Ethics and Conduct for Directors
8. Code of Ethics and Conduct for Subsidiary Directors
9. Corporate Privacy Policies and Procedures
10. Corporate Information Security Policies and Standards
11. Privacy Office Glossary of Terms
12. Privacy Office Decision Guidance & Tools
13. Human Resources HR 2.07 - Employee and Contingent Worker Classification Policy

VI. SOURCES/REFERENCES

This policy is based on the applicable federal and state Privacy laws and regulations.

VII. POLICY REVIEWERS

Person Responsible for Review	Title	Date of Review
Carrie O'Gara	Executive Director Corporate Compliance	3/7/25
Peg Griffiths	Executive Director Privacy Office	3/19/25

VIII. POLICY REVISION HISTORY

Description of Changes	Revision Date
Annual review with minor updates	5/8/25

IX. POLICY APPROVALS

Company Division, Department and/or Committee	By: Name	Title	Approval date
CASSIP	Jill Wolowitz	EVP, Chief Administrative Officer & Chief Ethics, Compliance and Privacy Officer	3/20/25
EPP Committee			5/8/25