HCSG Information Security Policy

Healthcare Services Group, Inc. and its subsidiaries (collectively, "HCSG") is committed to protecting its information technology systems, network, information, and data assets (collectively, its "IT System and Assets") from threats and seeks to minimize vulnerabilities to the privacy and security of its IT System and Assets. HCSG implements standards and processes relating to its management of information security controls and practices that are applied proportionately, based on a formal risk assessment (its "Information Security Policies").

HCSG's Information Security Policies are periodically reviewed based on the NIST Cybersecurity Framework. HCSG regularly monitors and measurers the performance of its IT System and Assets and its Information Security Policies. HCSG has procedures to ensure that any of its vendors and suppliers that create, utilize, or process HCSG's data take a similar, risk-based approach to information security.

HCSG's Information Security Policies are designed to:

- Safeguard its IT System and Assets, and data belonging to its customers, vendors, employees, and service providers;
- Monitor and support HCSG's compliance with regulations, standards, and legal requirements;
- Support the integrity of HCSG's IT System and Assets; and
- Support appropriate usage of HCSG's IT System and Assets.

HCSG is committed to the continued development and improvement of its IT System and Assets and its Information Security Policies by addressing identified risks and maintaining consistency with applicable law, frameworks, and guidance.

This Policy applies to any employee of HCSG that has authorized access to HCSG's IT Systems and Assets, or computer systems or networks connected to HCSG's IT Systems and Assets ("Covered Employees"). Each Covered Employee is required to comply with this Policy unless a prior exception request has been reviewed and approved by the Chief Compliance Officer. Failure to comply with this Policy could result in accidental or deliberate misuse of HCSG's IT System and Assets, which could increase the risk of security breaches and compromise HCSG's systems and services. Improper use of HCSG's IT System and Assets increases the risk of harm to HCSG's reputation, and may adversely impact HCSG's business, employees, suppliers, customers, and end users of HCSG's services. Compliance with this Policy minimizes the risk of breaches of confidentiality, malicious or accidental corruption of data, and supports our ongoing compliance with legal and contractual obligations.
Accordingly, HCSG IT System and Assets may only be used to support HCSG business and operations. Covered Employees may not use HCSG IT System and Assets for personal use,

unless authorized by their supervisor. Use of HCSG IT System and Assets must always be conducted in a professional manner.

The following actions are never permitted by Covered Employees when using HCSG IT System and Assets:

- Compromising the confidentiality, integrity, or availability of HCSG IT System and Assets.
- Use of threatening, obscene, profane, harassing, or offensive language or content.
- Gaming, personal file sharing, downloading or streaming music or other entertainment, or other similar activities.
- Work for another business, commercial ventures, or non-HCSG-sponsored activity.
- Advertising, purchasing, selling, or transacting non-HCSG business or initiatives.
- Any illegal activities.

In addition, Covered Employees must:

- Always follow HCSG policies.
- Help HCSG meet and maintain compliance with this Policy.
- Be aware of their role in supporting HCSG's Information Security Policies.
- Comply with relevant regulations, standards, and/or laws governing HCSG and its customers, third parties, and other applicable entities.
- Safeguard HCSG's assets in accordance with this Policy.
- Report any deviation from this Policy to the HCSG Help Desk. Individuals should report any deviation they discover or suspect immediately and must not engage in their own investigation or other activities unless specifically authorized.

Covered Employees who are found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action up to and including termination of employment.