

CODE OF CONDUCT



Message From Our CEO



SCP Health is dedicated to maintaining a culture of compliance. Our reputation, built on ethical behavior, honesty and integrity, is one of our greatest assets. Our commitment to safeguard this asset is supported by a continuously improving and effective Compliance Program.

The Code of Conduct has been approved by our Board of Directors and is the foundation that will ensure each of us is compliant with the laws and regulations pertaining to our daily work. The Code of Conduct will help us to make the right choices. I urge you to read carefully through this document and ask questions if you have any questions.

Each employee, provider, and agent of our Company is responsible for maintaining our corporate integrity and upholding our good name. We expect all employees, providers, and agents of the company to comply with the principles and guidelines laid out in the Code of Conduct and all policies and procedures implemented through our Compliance Program.

Considering the rapid change in healthcare today, it is increasingly important that we focus on compliance to ensure we can continue to provide the best care possible to our patients. With the continued commitment of our employees, providers and agents, I am confident our purpose and reputation will remain strong as we continue to serve millions of patients in the future.

Thank you for the work that you do every day!

Richard D'Amato
CEO

Table of Contents

Welcome from Compliance, Privacy and Information Security Officer.....	3
Corporate Compliance Program.....	5
Collaboration.....	8
Respect.....	10
Agility.....	22
Courage.....	23

Meet Your Compliance, Privacy and Information Security Officials



SCP Health is a committed advocate of compliance in all aspects of the Company. Whether it be protecting the privacy of our patients or safeguarding the proprietary information of the Company, or any one of a number of processes or data that we all touch every day in our work, a commitment to compliance exists. We all work hard and work together in the obstacles that confront us day-to-day, but we all also strive and must constantly endeavor to do the right thing. Therefore, keep doing what you are doing and take pride in your work and our Company!

Sarah Crass, ESQ
General Counsel & Chief Compliance Officer



We are in a time of increased governmental scrutiny and ever-changing regulation. We are committed to ensuring that our organization maintains a culture of compliance. Through our Compliance Program, we strive to ensure that our employees and providers are confident that they are doing the right thing. We support them in detecting non-compliance issues and immediately correcting any issues identified. In order to be successful and live our mission, we recognize that an effective Compliance Program is imperative.

Aimee Bertrand, MBA, CHC, RHIA
Vice President, Compliance



SCP Health's commitment to improvement and value-added services to patients, providers and facilities is further demonstrated through the establishment of its internal audit and Sarbanes-Oxley (SOX) programs. Independent of management, these programs provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. It includes objectives such as operational efficiency, safeguarding assets and financial statement reliability. Leadership is fully vested in these programs to mitigate risk and improve our internal control environment. However, remember, our internal control environment is only as good as the company culture set forth through our values: agility, courage, respect and collaboration that each of you exhibit every day!

Bradley Kohrt
Vice President, Internal Audit & SOX Compliance



At SCP Health, a patient's privacy and confidentiality remains top of mind throughout our various company touch points. We are made up of a vast team of hard working individuals that realize the high level of importance placed on our patients, along with the ever-changing electronic technology. There is a solid cornerstone of respect for patient privacy and confidentiality that is weaved into the Company's day-to-day operations. From our workforce onboarding process to annual HIPAA training to helpful privacy and security tips, our workforce stands tall against major healthcare companies. User access, auditing and timely reporting of privacy incidents supports the sense of priority, which contributes to the strength of our privacy program. Along with a sense of priority is a commitment to being accountable for handling our patient and company information with the utmost confidentiality.

Kathy Boone, RHIA
Privacy Officer & Compliance Manager



Our Company takes Information Security seriously, as we must protect our most valuable asset, the data stored within our network. Such data consists of ePHI (electronic Protected Health Information), PII (Personally Identifiable Information), and company data that is considered sensitive or confidential. Not only must we comply with the HIPAA Security Rule and PCI (Payment Card Institute) Data Security Standards, we must also guard against current and emerging Cybersecurity threats. Our greatest defense against a compromise of data and Cybersecurity threats is its workforce. By complying with Information Security policies and procedures, workforce members can help to significantly mitigate our risks. Information Security begins with YOU!

Sean Peltier

VP of Network Operations and Infrastructure & Information Security Officer

Our Corporate Compliance Program



This Code of Conduct (the “Code”) has been adopted by the Board of Directors (the “Board”) of Onex TSG/HPP Holding Corp, and is applicable to Onex TSG/HPP Holdings Corp. and all of its wholly owned subsidiaries and controlled affiliates (hereinafter collectively referred to as “Company”) and all Board members, directors, officers, employees, contracted healthcare providers, volunteers, interns and agents (“Team Members”) of Company regardless of location. This Code is designed to provide guidance to all Team Members in carrying out our commitment to legal and ethical behavior.

This Code is a critical part of our overall Corporate Compliance Program (“Compliance Program”) and discusses ethical and legal principles that must guide our work and relationships with patients, independent contractors, third-party payers, subcontractors, vendors, consultants, and each other. This Code is an integral part of how we achieve our purpose and ambitions.

Our Purpose:

- ▶ **We provide clinical leadership and all the requisite tools so that our providers can focus on the needs of patients.**
- ▶ **We help hospitals adapt, grow, and excel clinically so that they can better serve both patients and their communities.**
- ▶ **In doing so, we set out to make a positive difference across the entire continuum of care.**

Company is committed to compliance with all applicable federal and state laws, rules and regulations. This commitment permeates all levels of the organization. Our Compliance Program was created to ensure that we conduct our business with integrity and in accordance with applicable federal and state laws and our policies, to reduce the risk of misconduct, as well as to provide a safe environment for raising compliance concerns and questions. The Chief Compliance Officer oversees the Compliance Program and ensures compliance with our Code.

The Compliance Program, originally adopted by the Board of Directors in 1997, outlines what we do as an organization to comply with legal and ethical requirements, including the following:

- Setting integrity standards through the written policies, procedures, and our Code of Conduct;
- Communicating standards through awareness, education and training programs;
- Providing a process for reporting potential violations of laws, policies or our Code of Conduct;
- Conducting ongoing auditing and monitoring activities;
- Identifying, investigating, and responding to potential compliance problems;
- Performing routine sanctions checks to ensure we are not conducting our business with individuals and entities ineligible to participate in federal health care programs;
- Enforcing integrity standards and disciplining non-compliant actions; and
- Maintaining an organizational structure that supports the furtherance of the Compliance Program, including establishment of a Compliance Committee and appointment of a Chief Compliance Officer, who has an independent reporting relationship to the CEO and the Board of Directors.

This Code is the keystone of our Compliance Program and guides us in carrying out our daily activities within appropriate ethical and legal standards. This Code is intended to be comprehensive, easily understood, and serve as an important reference source for all Team Members.

Every Team Member has a responsibility to report the possible violation of this code, any Company policy, or any legal or regulatory requirement. Company will not tolerate retaliation against anyone for such reporting. Anyone who does not comply with this code may be disciplined up to and including termination.

This Code is an evolving document that will be updated periodically to respond to changing conditions and to reflect changes in law. However, this Code is not intended to cover every possible situation that may arise.

We have adopted a comprehensive set of compliance policies and procedures that expand upon the information presented in this Code and are available to every Team Member on the Employee and Provider Portals. It is the responsibility of each individual to be aware of all policies and procedures that pertain to his or her work and to follow those policies and procedures. Questions or issues regarding this Code or specific policies and procedures should be discussed with the Manager and Director of your department or the Compliance Department.

This Code of Conduct is available on Company website. This Code of Conduct is not intended to create any contractual rights to employment. For further information on the Corporate Compliance Program and its policies and procedures, please reference our Compliance Portal.

Culture of Excellence



Every Team Member has a responsibility to report the possible violation of this Code, any Company policy, or any law or regulation of which they become aware. Company will not tolerate retaliation against anyone for such reporting. Anyone who does not comply with this Code may be disciplined up to and including termination.

Each Department Manager and Director are also responsible for ensuring that each Team Member understands the Company's Compliance Program and the importance of Team Members **Collaboration** in fulfilling their responsibilities under this Code and the Compliance Program; in exercising **Respect** for financial matters, business conduct, workplace and employment practices; **Agility** in adapting to our evolving environment through education, training, auditing and monitoring processes, and ensuring Team Members have the **Courage** to report through open lines of communication and promotion of a non-retaliatory corporate environment. **Policy Reference: CCP-010 Manager and Director Responsibility**



Collaboration



Everyone is responsible for ensuring compliance! To assist you with this responsibility, our Compliance Program has been designed to ensure that there is an open line of communication between you and the Compliance Department should you ever become confronted with a situation that raises questions about legal or ethical business conduct.

Each department and/or office location has appointed a Compliance Representative to be a liaison between their team and the Compliance Department. The Compliance Representatives play a vital role in not only sharing compliance communications but also safeguarding their work locations. Thank you to all Team Members who have served or currently serving as a Compliance Representative. Your hard work and dedication are appreciated.

To effectively detect, resolve and prevent instances of noncompliance, it is very important, **as well as required**, that you immediately report any perceived or known violation of a law or regulation of our Code or policies to your immediate supervisor or to the Chief Compliance Officer, the Compliance Department or Compliance Hotline. Failure to report may result in disciplinary actions, up to and including termination.

We are committed to providing an environment that allows reporting in good faith without fear of retaliation. Our Compliance Department will evaluate all reports promptly, completely and fairly. You can report compliance concerns in one of the following ways:

You can speak with your immediate supervisor. We encourage you to first contact your immediate supervisor, who is in turn responsible for informing the Chief Compliance Officer and/or the Compliance Department of any concerns raised.

You can report directly to the Chief Compliance Officer or Compliance Department.

If you prefer not to discuss a concern with your supervisor, you may instead contact the Chief Compliance Officer and/or the Compliance Department directly and confidentially at: **compliance_officer@scp-health.com** or

Sarah Crass, Esq. General Counsel & Chief Compliance Officer 337-609-1147
Aimee Bertrand, VP Compliance 337-609-1404

You can call our Confidential Compliance Hotline or report via a secure website.

Call the 24 hour Confidential and Anonymous Hotline at: **1-877-778-5463**
or log on to our website at: www.reportit.net (Company username is SCPHEALTH -password HOTLINE70508)

If you report a compliance concern, be sure to include information that our Compliance Department will need to follow up, such as the location (where your concern occurred or is occurring), the date and time of the incident, the names and job roles of individuals involved in the concern, a description of your concerns and your name, *if you are comfortable letting us know*. **If you are not comfortable leaving your name, you may make an anonymous report by calling the above Confidential and Anonymous Hotline.**

Company shall always strive to maintain the confidentiality of a complainant's identity, regardless of the methods used to report suspected non-compliance. However, the complainant's identity may have to be revealed in certain circumstances, such as scenarios involving government or law enforcement authorities. The findings of a compliance investigation are confidential to protect all involved in the investigation process. As a result, details and specific findings of a compliance investigation will be shared only on a need-to-know basis. The Chief Compliance Officer ensures that all credible reports will be thoroughly and fairly investigated, and that appropriate action will be taken.

If you have a sincere belief that a violation may have occurred and make a report using any of the procedures provided in this Code, you will not be subject to retaliation. No adverse action will be taken against anyone for making a good faith report or for cooperating with a compliance investigation in good faith. We have a policy that protects against retaliation or retribution for reporting a compliance concern in good faith and cooperating with a compliance investigation in good faith. The non-retaliation policy ensures that no one is penalized for reporting what is honestly believed to be a compliance problem or for honestly participating in a compliance investigation. Forms of retaliation may include being fired, demoted, suspended, reprimanded, harassed, or in any way discriminated against for reporting a suspected violation. **Policy Reference: CCP-009 Non-Retaliation**

Although reported concerns may not always be correct, purposely falsifying or misrepresenting a report or making false statements during an investigation will not be protected under the Non-retaliation policy. False accusations or statements made in a report or during an investigation, including those made with the intent of harming or retaliating against another person, may result in disciplinary action, up to and including termination.

Although we have a policy that prohibits retaliation for reporting or cooperating in good faith, it is important to understand that no policy can protect you from applicable consequences if you have broken the law or violated our policies. Breaking the law or violating our Code of Conduct or our policies may result in disciplinary action up to and including termination, as well as possible federal and state actions and penalties.

We are committed to correcting wrongdoing, whether intentional or inadvertent, where it may occur in the organization, and to cooperating fully with government investigations.

Reported violations will be dealt with fairly, promptly and consistently in a manner that takes into consideration the seriousness of the violation and the conduct of individuals involved. Self-reporting is encouraged and will be considered when addressing the violation.

Respect



Company takes great care to ensure that billing to the government payors, commercial insurance payors and patients is accurate and conforms to all applicable federal and state laws, regulations and applicable guidance. We have implemented policies, procedures and systems to ensure that coding, billing and financial reports are handled with integrity and are accurate of the services provided by Team Members on behalf of Company.

In Financial Matters

A. CODING AND BILLING

Company has implemented policies, procedures and systems to facilitate accurate billing and coding of services provided by Team Members on behalf of Company.

Policy Reference: CCP-100 Billing for Medicare Services

We prohibit any Team Member from knowingly presenting, or causing to be presented, claims for payment or approval, which are false, fictitious or fraudulent. We are committed to timely, complete and accurate coding and billing, including the following principles:

- We bill only for services that are actually provided, documented, and ordered by a physician or other appropriately licensed individual who is a Team Member;
- We assign billing codes that we believe, in good faith, accurately represent the services that we provide and that are supported by documentation in the medical record according to regulatory requirements and guidelines;
- We implement good faith controls to prevent unbundling, coding errors, duplicate billing for the same service, and other government-published billing errors. Any improper coding as any error in coding (up or down) is not correct;
- We do not charge government payors in excess of our usual charges;
- We respond to billing and coding inquiries and timely resolve inaccuracies in previously submitted claims that are discovered and confirmed;
- We make every effort to ensure that Team Members who perform billing or coding services have the necessary skills, quality assurance processes and appropriate procedures to ensure that billings are accurate and complete; and
- We expect any subcontractors engaged to perform billing or coding services to have their own ethics and compliance program and code of conduct and agree to abide by ours.

B. FALSE CLAIMS ACT AND DEFICIT REDUCTION ACT

The Federal and State False Claims Acts and the Deficit Reduction Act protect government programs such as Medicare, Medicaid, and Tricare from fraud and abuse. It is a violation of the False Claims Act to knowingly submit, or cause another person or entity to submit, false claims for payment of government funds.

It is illegal to submit claims for payment to government programs that we know or should know are false or fraudulent. **No specific intent to defraud the government is required for a claim to qualify as a false claim.** The False Claims Act defines “knowing” to include not only actual knowledge, but also instances of deliberate ignorance or reckless disregard of the truth or falsity of a claim. Potential fines for violating the False Claims Act include a penalty of:

- Up to three times of the amount of the payment made on each false claim;
- Additional civil penalties ranging from \$11,181 to \$22,363 for each false claim; penalty ranges increase each year with inflation;
- Payment of the cost of the civil action by the entity or individual that submitted the false claims.

Filing false claims may also result in imprisonment, entering into a Corporate Integrity Agreement, or exclusion from participation in federal and state health care programs.

Policy Reference: CCP-105 Fraud and Abuse

WHISTLEBLOWER PROVISIONS - The False Claims Act allows people with evidence of fraud against the government to sue, on behalf of the United States Government, in order to recover the stolen funds. In some cases, the Government may join the whistleblower suit. If a whistleblower suit is ultimately successful, the person who initially brought the suit may be awarded a percentage of the recovered funds.

The False Claims Act also contains a provision that protects the whistleblower from retaliation by his or her employer. This provision applies to any employee who is discharged, demoted, suspended, threatened, harassed or discriminated against as a result of the employee's lawful acts in a whistle blower suit. It is our policy to extend Team Members all protections required by the False Claims Act.

In addition to the Federal False Claims Act, a number of states also have False Claims Acts with similar penalties that work to discourage fraud perpetrated against state governments. The Deficit Reduction Act of 2005 offered states the opportunity to retain 10% of any amount recovered through false claims if they enacted their own False Claims Act requirement that were comparable to the federal statute.

We are committed to submitting claims that are accurate and truthful. If you know of a false claim, contact your supervisor immediately, who is responsible for notifying the Chief Compliance Officer. You can also report concerns directly to the Chief Compliance Officer, the Compliance Department or call the Confidential Compliance Hotline 1-877-778-5463. Failure to notify the Chief Compliance Officer and or the Compliance Department of compliance violations may lead to disciplinary action, up to and including termination.

Policy Reference: CCP-016 Whistleblower

C. FINANCIAL ACCOUNTING SYSTEMS

The financial and tax accounting systems of Company are maintained in accordance with generally accepted accounting principles, subject to annual independent audit. Our system of internal controls is designed to provide assurance that all financial transactions are properly and timely accounted for and recorded.

Team Members involved in creating, processing or recording financial information are expected to take responsibility for its integrity.

Team Members may not be involved in the submission of false invoices or expense reports, the forging or alteration of checks or misdirection of payments, the unauthorized handling or reporting of transactions, the creation or manipulation of financial information so as to artificially inflate or depress financial results, or any improper or fraudulent interference with or coercion, manipulation or misleading of the auditors or the Audit Committee of the Board of Directors.

To identify financial and fraud risk, the Company has a Sarbanes-Oxley (SOX) program. The SOX program utilizes a top-down, risk-based approach based on the COSO 2013 framework. SOX program deliverables and Steering Committee are designed to support the annual SCP CEO and CFO certification:

- State the responsibility of Management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
 - Also, note that financial reporting includes all aspects of Financial Reporting including income statement, balance sheet, cash flows and footnotes and disclosures.

To support this annual certification, SOX process and control owners are responsible for remediating control deficiencies in a timely manner in accordance with an agreed upon plan and date.

In Business Conduct

A. STARK LAW

Team Members shall be required to abide by the Federal Physician Self-Referral Law, commonly referred to as the “Stark Law”. In general, the Stark Law prohibits contracted healthcare providers from making referrals for certain designated health services payable by Medicare to entities with which the physicians themselves or their immediate family members have a financial relationship, unless an exception applies. A financial relationship can take the form of a direct or indirect ownership either interest or compensation arrangement. Violations of the Stark Law can result in repayment of all claims made by improper referrals, Federal False Claims Act actions and penalties, and exclusion from the Federal health care programs. As such, compliance with an exception is important.

If you have any questions about a Stark Law exception or other Stark Law concerns, please contact the Compliance Department.

B. ANTI-KICKBACK STATUTES

The Federal Anti-Kickback Statute prohibits persons from knowingly and willfully soliciting, receiving, offering or paying any remuneration, directly or indirectly, overtly or covertly, in cash or in kind, in return for or to induce referring an individual for the furnishing of, purchase, leasing, ordering, or arranging for, any item or service paid for in whole or in part under a state or federal health care program. There are many similar state laws. Violation of the Anti-Kickback Statute is punishable by criminal penalties, which can include exclusion from participating in federal healthcare programs; fines; and/or jail time. Further, violation of the Federal Anti-Kickback statute can result in Federal False Claims Act actions and penalties and exclusion from the Federal health care programs.

It is our policy not to offer or solicit anything of value to or from someone for referral of patients, nor to accept or offer kickbacks for any service or product. We provide education on the relevant proscriptions and prohibited activities that may result in a violation of these laws.

Strict adherence by Team Members to the letter and spirit of the Stark Law, Anti-Kickback Statute, and Medicare/Medicaid regulations is required. No one should assume that the Company’s interest ever requires any other course of conduct. In addition to disciplinary action by Company, as noted above, civil and criminal penalties may be imposed for non-compliance.

If you have any questions or concerns about compliance with these laws, please contact the Compliance Department.

C. EMERGENCY MEDICAL TREATMENT

Team Members who provide services in hospitals are required to abide by the Emergency Medical Treatment & Active Labor Act ("EMTALA"). Providers and non-clinical Team Members are assigned mandatory EMTALA training when they onboard, then annually thereafter. Educational information is also provided regarding such regulations and any changes thereto.

It is our policy that, where applicable, Team Members who are healthcare providers located in hospitals shall provide an appropriate medical screening examination for all individuals and necessary stabilization for any patient in labor or with an emergency medical condition, without regard for an individual's ability to pay. Patients requiring transfer to another facility shall be transferred in strict compliance with State and Federal EMTALA requirements. Failure to comply with these requirements may result in fines being imposed on both the healthcare provider and the hospital. **Policy Reference: CCP-004 EMTALA**

D. PRIVACY OF PATIENT INFORMATION

Patients and their families trust us with highly personal and sensitive information regarding their medical conditions. We collect patient information, including medical conditions, history, medical and family illnesses, in order to provide quality care. Team Members are not permitted to access patient information internally or use or disclose patient information outside the organization, except as necessary to perform our jobs, serve the patient, or required by law. We are committed to complying with state and federal privacy laws and to assisting patients with exercising their patient privacy rights.

We have adopted policies and procedures, which reflect the requirements of the Health Information Portability and Accountability Act of 1996, as amended ("HIPAA"). We have also adopted policies and procedures, which reflect the requirement of protecting electronic health information as required by the Health Information Technology for Economic and Clinical Health Act ("HITECH").

Under our Notice of Privacy Practices, patients can expect their privacy will be protected. No Team Member has a right to any patient information other than that necessary to perform his or her job. Our policies focus on protecting individual's health care information that is accessed, used or disclosed in providing healthcare treatment and fulfilling billing requirements and health care operations of the health care provider ("Protected Health Information"). Although Company is not engaged in activities that define it as a Covered Entity, under HIPAA, Company may have separate direct and indirect subsidiaries that perform functions that fit the definition of a Covered Entity.

Companies may be designated as an "Affiliated Covered Entity", which permits the affiliated legally separate organizations to comply with one set of policies and procedures, appoint one Privacy Officer, administer common training programs, use one Business Associate Agreement, provide one Notice of Privacy Practices, etc. Those Companies classified as an Affiliated Covered Entity may share Protected Health Information among other entities classified as Affiliated Covered Entities for the performance of health care obligations. Any legally separate entity of Company that is not classified as an "Affiliated Covered Entity" may not receive or utilize Protected Health Information without patient authorization, unless otherwise allowed by law.

Our Compliance Department monitors electronic patient records to determine who is accessing the record and whether the access is consistent with job functions. Company privacy and security policies require:

- We access, use and disclose only the minimum amount of patient information necessary to perform our jobs;
- We do not discuss patient information with others who do not have a job-related need to know, including co-workers, colleagues, family and friends;
- We do not share our user IDs or passwords to our electronic systems and log-off when we step away from our computers; Note: what is done under your ID/password is your responsibility;
- We assess our surroundings when speaking with or about patient health information to ensure privacy;
- We verify written patient information to ensure that we do not mix one patient's information with another's, that fax numbers and email addresses are accurate and entered correctly before sending;
- We dispose of written patient information in confidential disposal bins, and we contact IT for proper disposal of electronic patient information;
- We encrypt all emails that contain patient health information, and we do not put patient health information in the subject line;
- We timely report all privacy concerns or potential privacy policy violations immediately to our Privacy Officer within the Compliance Department.

We are committed to ensuring the confidential and secure treatment of Protected Health Information maintained in both paper and electronic media. We have implemented policies and procedures to: limit uses and disclosures of patient information; ensure that no patient health information is disclosed unless permitted under HIPAA; enter into business associate agreements with those entities with which we share patient health information; limit access to patient health information to those individuals that need the information to perform their job; verify the identity of persons seeking patient health information; and address patient's rights with respect to their own health information.

The laws apply both to Company and to you as an individual, even after you no longer are a Team Member. Patient privacy laws include serious consequences for failing to protect patient privacy. Additionally, violating our privacy and security policies can lead to disciplinary actions, up to and including termination, financial penalties and reputational impact. Any questions regarding proper handling of patient health information should be addressed to the Privacy Officer. **Policy Reference: See HIPAA Privacy Policies posted on Compliance and Provider Portals**

E. CONFLICTS OF INTEREST

It is our policy that no employee should place himself or herself in a position where their action, personal interest, or the activity or interest of those for whom they act are, or are likely to be, in conflict with the interests of Company. The purpose of this policy is to assist Company and employees in avoiding situations where personal activities and financial affairs may conflict with their responsibility to act in the best interests of Company. There is no intent to invade individual privacy, but rather to identify possible problems or areas of concern that could be resolved if revealed.

Some examples of a conflict of interest include:

- Having an interest in or financial relationship with a vendor with which Company does or proposes to do business with or a competitor of Company;
- An employee using their position within Company to obtain personal benefits, or profit;
- Accepting gifts, payment or free services from vendors who seek to do business with Company, or;
- Conducting investment activity using confidential information obtained while working at Company.

Employees will receive an annual disclosure form and are expected to disclose any circumstances that could be perceived as a conflict of interest. Disclosure allows for amicable resolution should a conflict of interest exist.

Discussing any potential conflicts of interest with the Compliance Department in advance of entering into an arrangement, accepting a gift, etc. is best practice.

Policy Reference: CCP-018-Conflict of Interest

GIFTS AND BUSINESS COURTESIES

It is our policy that Team Members will maintain high ethical standards regarding the offering and acceptance of business gifts. Offering or accepting personal gifts may influence our decisions or the decisions of others and may constitute a conflict-of-interest. The appropriateness of offering or accepting gifts depends on the specific circumstances of the gift and who is offering and receiving it. Each Team Member needs to be sure that even permitted business gifts do not damage our reputation for integrity. Please refer to Company's *Corporate Ethics: Gift Policy* to ensure that your actions comply with our policies. An effort should also be made to ensure that any gift we extend meets the business conduct standards of the recipient's organization. If you are unsure, please contact the Compliance Department before offering, soliciting, giving or receiving such items. **Policy Reference: CCP-017 Anti-Bribery and Gifts Policy**

USE OF RESOURCES AND ASSETS

Our assets and resources are to be used for accomplishing our legitimate business purposes only and not for the personal interest of an individual Team Member. Team Members are prohibited from the unauthorized use or taking of our equipment, supplies, materials, or services. As a rule, the personal use of any Company asset without prior supervisory approval is prohibited. The occasional use of items where the cost to Company is insignificant is permissible. One's supervisor must approve any Company assets used for community or charitable purposes in advance. Any use of Company resources for personal financial gain unrelated to the Company's business is prohibited.

CORPORATE OPPORTUNITIES

Team Members are expected to advance the Company's legitimate business interests when the opportunity to do so arises. Team Members may not:

- Take for themselves (or direct to a third party to) a business opportunity that is discovered through the use of the Company's property, information or position or indeed any other opportunity which it reasonably believes may be of interest to Company,
- Use the Company's property, information or position for personal gain or compete with the Company.

Team Members owe a duty to Company to advance its legitimate interests whenever the opportunity to do so arises.

F. ACCURACY OF RECORDS AND DOCUMENT RETENTION

You are responsible for the integrity and accuracy of the records produced in the course of performing your work for Company. Accurate records and the integrity of our data support the business decisions and actions taken by Company.

We are committed to maintaining our business records in accordance with federal and state law. Such records are to be retained, stored and destroyed in compliance with our records retention and destruction policies. Business records include all documents and data created internally or externally on behalf of Company, whether in paper or electronic format. It is a violation of policy to alter, falsify, or tamper with Company records.

Policy Reference: CCP-026 Record Retention

G. CONFIDENTIAL BUSINESS INFORMATION

Confidential information about our organization's strategy and operations is a valuable asset. Although you may use confidential business information as necessary to perform your job, it must not be shared with others outside the organization or internally with those who do not need to know about the information to perform their jobs. Confidential and proprietary business information covers anything related to our business or operation that is not publicly known, such as personnel files, wage and salary information, financial information, billing and pricing information, strategic plans, projected earnings, information related to investigations, disciplinary actions, information related to acquisitions or joint ventures, and policies and procedures. Company's methods of operation, databases, and financial condition are considered proprietary and confidential business information.

Even when you are no longer a Team Member, you are still bound to maintain the confidentiality of information viewed, received, or used during the course of your relationship with the organization. Copies of electronic files of any confidential or proprietary information in your possession when you leave the organization must be returned at the end of your relationship with Company.

If you are in doubt about whether information you are being asked to share is confidential or proprietary, or if you know it is confidential and proprietary but are not sure about whether the request is legitimate, contact your supervisor or the Compliance Department. Releases of this type of information shall take place only with the consent of Executive Leadership, pursuant to a confidentiality and non-disclosure agreement, or if otherwise required by law, such as to comply with a court order.

Media Inquiries: It is important for Team Members to know that they are **not** authorized to speak to the media on behalf of the Company. All media inquiries should be referred to Company Spokesperson, Maura Nelson, VP Marketing & Communications. All inquiries should be emailed to the following: maura_nelson@scp-health.com and Marcomm@scp-health.com.

H. INFORMATION TECHNOLOGY & RESOURCES

Company has made significant investments in information technology systems used to manage the data in its business operations. We utilize software and hardware systems designed to protect the Company's electronic records from access by unauthorized individuals or entities, malicious destruction, and to protect the integrity and confidentiality of data during transmission. Policies and procedures are in place to ensure routine maintenance and upgrading of these systems. Users should be aware that certain electronic systems are monitored for inappropriate use and that not all systems provide confidential transmission of information. If confidential electronic transmission is required, users should contact our Information Technology Department to determine the proper method of transmission.

Our Security Officer oversees the management, implementation, and monitoring of our information systems. Use of Company owned and provided computer resources, telephone services, or supplies for other than for business use is not permitted. Our Team Members use software program for word processing, spreadsheets, data management and many other applications. Software products purchased by us are covered by some form of licensing agreement that describes terms, conditions and allowed uses. It is our policy to respect copyright laws and observe the terms and conditions of any license agreements. You are expected to abide by all copyright regulations and user license requirements, failure to do so may result in civil and criminal penalties. Again, if you have questions regarding compliance with copyright laws or license agreements, please contact the Compliance Department.

Policy Reference: See Information Security Policies posted on the Compliance and Provider Portals

I. REQUESTS FOR INFORMATION PURSUANT TO AN INVESTIGATION OR LEGAL PROCEEDING

We promptly and appropriately respond to requests for information pursuant to a government investigation, requests for information, or legal proceeding. These requests may come in the form of a subpoena, summons, warrant, letter or verbal request. Only the CEO, General Counsel and the Chief Compliance Officer or someone who is otherwise authorized by one of the foregoing, are authorized to accept these documents on behalf of Company.

Accepting or acting on these requests may expose Company, and sometimes you as an individual, to significant fines or other types of criminal, civil, or administrative penalties. If you are asked to accept a legal document or to share information of any kind for any reason, immediately consult with your supervisor and/or the Compliance Department.

Policy Reference: CCP-008 Government Requests Investigations

J. POLITICAL AND CHARITABLE ACTIVITIES

Company encourages participation in charity and community events; however, Team Members should be clear that they are acting or speaking on their own behalf and not on behalf of Company when engaging in political and charitable activities, unless they are authorized by the Company to act on its behalf. Donations of Company funds or assets and the use of the Company name or logo is **not** permitted unless you have proper written authorization. **Policy Reference: CCP-014 Corporate Donation and Sponsorship Policy**

In the Workplace and Employment Practices

We value our employees and strive to provide a comfortable and safe work environment. To ensure that this goal is achieved, Company has adopted policies with respect to employment matters, employee rights, and benefits. Any violations of such policies should be directed to Human Resources. Access to personal information about employees is restricted to people with a "need to know" within Company and will be transmitted to other employees or third parties only for legitimate business need or as required by law.

A. HARASSMENT/DISCRIMINATION

Company strives to provide a productive work environment in which all of our Team Members can contribute at their highest levels. Accordingly, we prohibit harassment and discrimination of any kind, whether the harasser or victim is a supervisor, co-worker, supplier, customer, agent, or guest of Company.

Sexual harassment is defined as any unwelcome or unwanted advances, requests for sexual favors, verbal, visual or physical conduct of a sexual nature, when:

- Submission to or rejection of this conduct by an individual is used as a factor in decisions affecting hiring, evaluation, retention, promotion or other aspects of employment; or
- This conduct reasonably could be expected to and does interfere with any individual's employment or creates an intimidating or hostile work environment.

Sexual harassment is a violation of law and applies not only to each of us in our work environment but also to all locations where we present ourselves. A team member who feels that he or she has been subject to harassment should immediately report the matter to their supervisor or to Human Resources or should call the Confidential Compliance Hotline.

Company pledges that every Team Member will be treated with dignity and respect and will be judged based on his or her qualifications to perform a job, without regard to race, creed, gender, religion, national origin, age, disability, or veteran status. Discrimination in any form is a violation of law.

Company has adopted certain other policies and procedures with respect to other human resource issues and our Team Member benefits. These additional policies are set forth in the Human Resources Manual provided to each Team Member upon commencement of their relationship with Company.

Please contact the Human Resources Department with any questions regarding these policies or benefits. **Policy Reference: See Human Resources Manual**

B. WORKPLACE VIOLENCE

Company has a **zero** tolerance for threats or acts of violence in the workplace. Workplace violence includes physical assaults, actions, or statements that give us reasonable cause to believe that our personal safety or the safety of others may be at risk. Team Members who engage in physically abusive and/or violent behavior (even those in jest) shall be subject to disciplinary action up to and including removal from Company, termination of employment or contract, and/or referral to appropriate law enforcement agencies. If you believe a certain behavior is physically threatening or intimidating, you should immediately report to your immediate supervisor or, in cases involving behavior of your immediate supervisor, the next-level supervisor, or the Human Resources Department.

In cases of imminent danger of bodily harm, call the Human Resources Department and then call a second person to assist, as needed. Reported events will be investigated and, if warranted, appropriate support will be provided to the victim(s). Company will track these reports and evaluate trends to develop and implement precautionary measures.

Policy Reference: See Human Resources Manual

C. WORKPLACE HEALTH

In our continuing commitment to an environment of good health, we have designated various Company offices as smoke free. Smoking is not permitted anywhere inside Company buildings or within defined geographical areas outside the buildings, as set forth in our *Smoking Policy*, of the Human Resources Manual.

It is our policy to provide a safe and drug-free work environment for our Team members. The use of illegal drugs and abuse of controlled substances in the workplace is prohibited. As a condition of employment or affiliation with Company, any involvement in the unlawful use, sale, manufacture, distribution or possession of controlled substances, illicit drugs and/or unauthorized use of alcohol in the workplace or working under the influence of such substances is prohibited. We encourage Team Members with alcohol or drug dependencies to seek treatment and/or rehabilitation. Team Members who experience problems with alcohol or other drugs may contact Human Resources for confidential assistance or referral to appropriate resources, including Company's Employee Assistance Program (EAP) provider, as set forth in the *Drug-Free Workplace Act Policy*, of the Human Resources Manual.

D. WORKPLACE SAFETY

As part of our overall commitment to maintain a safe environment for our Team Members and others, we strive to keep our facilities physically secure. We are issued security badges that must be worn above the waist at all times. It is your responsibility to keep your badge in your possession and **not** let any other person borrow it. If it is lost or stolen, notify your manager, the Human Resources Department and/or the Compliance Department immediately. In addition, be aware of your surroundings and report any suspicious person or activity to your manager, the Human Resources Department and/or the Compliance Department.

We have an extensive safety program to reduce the risk of injury to Team Members and visitors and to assure compliance with applicable federal, state and local codes and regulations, as applied to the building we inhabit and services we provide. It includes making sure that our department Managers and Directors have appropriate information and training to develop safe working conditions and safe work practices within their area of expertise; using knowledge or safety principles to educate staff, design appropriate work environments, purchase appropriate equipment and supplies and monitor the implementation of the processes and polices; and regularly evaluating the environment for work practices and hazards to respond to identified risks, hazards and regulatory compliance issues. If you have any questions about specific policies that apply to your job or tasks, please speak with your immediate supervisor.

E. TEAM MEMBER SCREENING

We do not contract or employ individuals or bill for services rendered by an individual or entity that are excluded or ineligible to participate in federal healthcare programs; suspended or debarred from federal government contracts; or not reinstated in a federal healthcare program after a period of exclusion, suspension, debarment or ineligibility.

It is also our policy to prevent Company from delegating discretionary authority to an individual or entity that may have a propensity to engage in illegal activities. We conduct an initial screening prior to start date and monthly re-screenings of all Team Members against established governmental databases of such excluded and ineligible persons, per OIG exclusion guidance. Our policies address the procedures for timely and thorough review of such lists and appropriate enforcement actions. Each prospective Team Member is required to sign a release/authorization with respect to this policy.

Additionally, as a Team Member you are required to immediately report to Company if you become excluded, debarred, or ineligible to participate in federal healthcare program; or if any proceedings are instituted against you that may result in sanction by or exclusion from a government sponsored healthcare program.

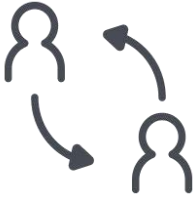
Policy Reference: CCP-012 Screening for Excluded Individuals/Entities

F. PROFESSIONAL LICENSING

Company will not employ or contract with individuals that do not hold mandated professional credentials. Individuals retained by Company that require professional licensure, certifications or other credentials are responsible for continuing to maintain those licenses, certifications, or credentials, in accordance with applicable federal or state regulations. Company may periodically require evidence of the status of such credentials or licenses.

We encourage our Team Members to pursue professional certifications.

Agility



Company seeks to promote a corporate environment of compliance with all applicable legal requirements and to assure that the standards set forth in this Compliance Plan are maintained. The Chief Compliance Officer, with the assistance of Department Managers and Directors will continue to assist Team Members in adapting to our evolving environment through education, training, and policies and procedures.

Education and Training

Every Team Member, upon engagement, is required to participate in general compliance education and to confirm that he or she:

- Has completed this education;
- Has read and understands the Code of Conduct, has access to the Code, and Company's Compliance Policies and Procedures; and
- Understands that compliance with this Code, Compliance Policies and Procedures and the law, is required at all times that he or she is a Team Member.

Existing Team Member are required to complete annual compliance training along with relevant healthcare laws and regulations.

- Team Members with job functions in areas identified as highly regulated, or at a higher risk for intentional or inadvertent wrongdoing, will receive more intensive education and training (e.g., coding, billing, and medical documentation).
- Team Members will also receive on-going training as determined by the Compliance Officer, with assistance from the Quality and Compliance Committee.
- Team Members may also receive additional, specific compliance training which focuses on the specific policies and procedures relevant to the services provided by the Team Member

Timely completion of training is required and part of Team Members annual performance evaluation. With the assistance of the Managers and Directors of the various departments, all compliance training will be tracked and reported, as necessary, by the Compliance Department. **Policy Reference: CCP-101 Education and Training**

This Code, and/or the policies and procedures may be revised, amended, or supplemented. A copy of all revisions, amendments or supplements shall be provided to all Team Members. This Code, and policies and procedures are also always available to Team Members on the Employee and Provider Portals and the Company website.

As a multi-state business, Company is subject to the laws and business requirements of the states in which it operates. Wherever you may be located, you are responsible for conducting business activities in compliance with this Code and the laws of the state in which you work and live. When you believe a conflict exists or may exist between this Code and the laws of a particular state, you should bring that conflict to the attention of the Compliance Department.

Courage



In an effort to ensure that the Compliance Program is an effective program, Company not only encourages all Team Members to raise conduct or ethical concerns to an immediate supervisor or the Compliance Department, but Company also strives to effectively detect, resolve and prevent instances of noncompliance.

Monitoring and Auditing

Company believes that establishing internal control procedures, active self-monitoring and periodic external audits permit us to identify areas of risk and provide assurances that we are conducting our business in compliance with laws, regulations and our own policies. Company has adopted certain policies and procedures with respect to specific monitoring and auditing of business areas that are strictly regulated or that the Board has identified as having a higher level of risk for intentional or inadvertent wrongdoing.

In addition, the Company has established an internal audit function. The objective of the function is to provide independent, objective assurance and consulting activity designed to add value and improve the Company's operations. The Internal Audit Plan is developed based on a prioritization of the audit universe using a risk-based methodology, including government guidance, prior audit findings, and input of senior management, the Audit Committee and the Board. **Policy Reference: CCP-013 Auditing and Monitoring**

Open Lines of Communication

Company has implemented tracking, documentation, and oversight mechanisms to ensure that reports of suspected noncompliance are fully and promptly investigated and addressed.

Company has also made available to Team Members a Confidential Compliance Hotline (1-877-778-5463), where Team Members are permitted to report matters on an anonymous basis.

Matters reported through the Compliance Hotline or other communication sources that suggest violations of compliance policies, federal, state, or private payor health care program requirements, regulations, or statutes will be documented and investigated promptly to determine their veracity and remediated timely.

Policy Reference: CCP-011 Compliance Hotline

Decision Making

Our Code of Conduct is designed to help you make ethical business decisions. It is not, however, designed to address every issue. You may face a situation where the right course of action is unclear. Asking the following question will help you maintain the mission and values of Company:

- Is it in consistent with our mission and values?
- Is it illegal?
- Is it unethical?
- Could it harm patients?
- Could it harm fellow Team Members?
- Could it harm government programs?
- Could it harm our financial health?
- Would our organization be compromised or embarrassed if it became public knowledge?
- Is it unfair or inappropriate?
- Could it adversely impact our organization if everyone did it?
- Is it in consistent with our policies or our Code of Conduct?

If the answer to any of the above questions is “yes” do not do it. If you are still unsure what decision to make or what action to take, talk to your supervisor or contact the Chief Compliance Officer. It is critical that our Compliance Program is effectively communicated throughout all levels of the organization.

Compliance is the responsibility of each Team Member. The Compliance Department encourages you to provide constructive input regarding its Compliance Program and our Code of Conduct. If you have and comments, suggestions or questions, please submit them to the Compliance Department.

SCP Health Compliance Department

Contact us: 800-893-9698 ext. 1117

General Counsel and Chief Compliance Officer

Sarah Crass, Esq. 337-609-1147

VP Compliance

Aimee Bertrand, 337-609-1404

Report via our 24 hour Confidential & Anonymous Hotline:

1-877-778-5463 or **via our secure website at:** www.reportit.net

E-mail us:

compliance_officer@scp-health.com

privacy_officer@scp-health.com

Mail:

Attn: Compliance Department

P.O. Box 82368

Lafayette, LA 70508-2368