SCM | Associates

Job Description

Position: Administrative Assistant I

Department: Case Management

Reports to: Manager of Case Management

Summary

The administrative assistant assists Case Managers as needed with a variety of administrative duties. Duties including, but not limited to such as performing, compiling, and maintaining records of business transactions and office activities in close coordination with other staff members.

Responsibilities and Duties

Responsibilities may include the following:

- Types and sends general office correspondence, letters, and forms
- Provides general administrative support to the Case Managers, including screening and directing phone calls, calendar, phone calling, and travel
- Performs general information research as assigned and summarizes it in verbal and/or written form
- Performs routine case management tasks assigned by the Case Manager, including scheduling patient appointments, arranging for associated needs such as transportation and translation, and submitting authorization forms
- Enters and maintains case data in databases and other office software and transfers information among programs, including prepopulating reports
- Organizes travel and service arrangements and other engagements and communicates with service providers
- Documents in writing all work activities and time required to perform them
- Communicates effectively via phone, e-mail, or fax with company personnel, vendors, customers, and clients
- Notifies management staff of any issue related to quality of service provided or legalities
- Performs other related duties as assigned in accordance with the necessary job function

Supervisory Responsibilities

This position has no supervisory responsibilities.

People Contact

This position requires regular contact both within the company and outside the company in order to carry out company policies and procedures. Requires abilities of persuasion and co-operation. Often deals with persons of equal or higher rank.

Decision Making

This position requires the use of judgment to plan and execute the workload. General decisions are made to solve problems by selecting a course of action that is within the policies and procedures of the company. Uses good judgment in referring problems to manager.

Supervision Received

This position exercises some latitude in planning and executing the workload, but works closely with the supervisor. Completed work is reviewed in terms of timely and effective performance of responsibilities.

Minimum Position Qualifications

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Education and/or Experience:

- High school education
- Prior computer experience
- Two years related experience and/or training or equivalent combination of education and experience

Language Skills:

- Ability to read, analyze, and interpret information

- Ability to effectively present information and respond to questions from customers and managers regarding the case management process
- Ability to speak effectively on the phone to customers

Mathematical Skills:

- Ability to add, subtract, multiply, and divide in all units of measure, using whole numbers, common fractions, and decimals
- Ability to compute rate, ratio, and percent and to draw and interpret bar graphs

Reasoning Ability:

- Ability to apply common sense understanding to carry out instructions furnished in written, oral, or diagram form
- Ability to deal with problems involving several variables in standardized situations

Computer Skills:

- Knowledge of database software, internet software, and Microsoft word processing and spreadsheet software

Certificates, Licenses, Registrations:

- Valid California driver's license and valid automobile liability insurance

Other Skills and Abilities:

- Ability to organize and evaluate workload and prioritize projects
- Ability to meet deadlines
- Ability to complete multiple, simultaneous projects with accuracy and efficiency
- Ability to problem solve
- Detail orientation

Physical Demands

The physical demands described are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee regularly is required to sit and talk or hear. The employee occasionally is required to stand and walk. The employee frequently is required to use hands to finger, handle, or feel and to reach with hands and arms. The employee occasionally is required to stoop, kneel, or crouch. The employee occasionally must lift

and/or move up to ten pounds. Specific vision abilities required by this job include close vision (clear vision at 20 inches or less) and ability to adjust focus.

Work Environment

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions.

The noise level in the work environment is usually moderate.

At Will Employment

Employment at SCM Associates, Inc. is based on mutual consent, and both the employee and SCM have the right to terminate employment at will, with or without cause, with or without advance notice.

Acknowledgement

The job description has been discussed with me, and I have received a copy of it.

Employee Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

Schedule 1.1: Confidentiality and Information Security Requirements

(a) Definitions

1. SCM Confidential Information:

   1.1. Includes, without limitation, a Client's health information (also known as Personal Health Information), including but not limited to medical records, monthly reports, working notes, billing information and any Contract-related information for a particular Contract (or case). It also includes, without limitation, SCM's and SCM's Customers' business policies, hiring, security and other practices, strategies, concepts, methodologies, operations, products, services, Customer lists, claims information and pricing information.

   1.2. May be provided in any form, including without limitation orally, written paper form or electronically (which includes, but is not limited to, emails, computer disks, video disks, CDs or tapes, whether machine or user readable).

2. Laws:

   2.1. Are any and all laws, rules and regulations of any federal, state or local authority applicable to the performance of SCM case management services, during the term of employment and for so long thereafter as the employee has access to or possession of SCM Confidential Information.

   2.2. Include laws that relate in any way to the privacy, confidentiality or security of Personal Health Information, including without limitation: security breach notification laws; laws imposing minimum data security requirements, laws requiring the secure disposal of

records containing certain personal information; laws governing the use and transmission of social security numbers; and any legislation and/or regulations implementing or made under or pursuant to or amending or succeeding all such laws.

3. Security Incident: any unauthorized acquisition (including loss or theft), destruction, modification, use, disclosure of or access to SCM's Confidential Information (including, without limitation, repair services, an authorized user acting outside the scope of their authority, system attacks, penetrations, denial of service attacks, misuses of access and instances of hacking or other unauthorized access or intrusion, virus dissemination or intrusion or unauthorized scans of any part of a network or computing resources or of any SCM Confidential Information installed, running, processed, stored, or maintained therein).

(b) Data Access and Background Checks

1. Before being granted access to SCM Confidential Information of any kind, each employee must complete the account provisioning processes and security requirements of SCM and those of any applicable SCM Customers.

2. As part of SCM's account provisioning process, appropriate waivers/consents will be obtained from the employee for a background check, including any waivers/consents needed to share the results with SCM Customers where required, and SCM will obtain a background check (a) in accordance with applicable laws; and (b) including, at a minimum, state, federal and county felonies and misdemeanors occurring within seven (7) years from the date the background check is performed, which date shall not be more than twelve (12) months earlier.

3. In the event that a background check indicates the commission of a felony or misdemeanor, SCM will conduct an individualized assessment and make the appropriate determination up to and including denying or removing approval for the employee to participate in SCM case management services.

4. Except where access by SCM's IT team is permitted by SCM and its Customers, the employee is strictly prohibited from sharing SCM accounts or its Customers' accounts with anyone, as these accounts are designated solely for single individuals.

(c) Confidentiality

1. SCM Confidential Information shall be maintained, on any device or on paper, solely as is necessary to perform case management services, and subject to all applicable Laws. The employee will additionally comply with any Customer limitations as to its Confidential Information. Any Confidential Information maintained on paper will be kept in a secure location accessible only by authorized SCM employees, such as a locked file cabinet.

2. The employee will follow current SCM and Customer requirements regarding structure and confidentiality of account access information such as usernames and passwords, including keeping any record of the account access information only in a secure location that cannot be accessed by others.

3. The employee will confirm recipient information such as phone number, fax number, or email address prior to sending any communication containing SCM Confidential Information.

4. The employee will send communications containing SCM Confidential Information only to individuals with a reasonably necessary business reason to receive them, and will confirm appropriate security at the recipient end, including but not limited to a fax machine to which only the authorized recipient has access or where the recipient is expecting the fax and will not leave the item unattended.

5. The employee will send communications regarding SCM Confidential Information only through designated means and subject to designated requirements, including but not limited to the encrypted email accounts provided by SCM and its Customers and the use of fax cover sheets with information specified by SCM or the Customer. Forwarding or other transfer of SCM Confidential Information from SCM or Customer accounts to other accounts, including but not limited to personal accounts or accounts used at other companies, is strictly prohibited.

6. The employee will ensure that any paper communications containing SCM Confidential Information are sent in opaque envelopes with no "see-through" and with no Confidential Information visible through an envelope window.

7. The employee will securely destroy all SCM Contract-related information upon request by SCM or its Customer and within 30 days of SCM submitting the last invoice for that Contract to the Customer. The employee will securely destroy or return to SCM all other SCM Confidential Information upon request by SCM or its Customer and at separation from employment by SCM, according to SCM's current policies and procedures, including uploading required information to SCM and Customer systems, return or physical shredding of all paper documents, and secure e-shredding of electronic copies according to SCM's current policies. SCM may require a written certificate from professional shredding services or e-shredding programs, or an attestation regarding other forms of secure destruction.

(d) Security Incidents and Auditing

1. The employee will notify SCM immediately, and in any case within 12 hours, by calling SCM's President/CEO, Manager of Case Management, or Business Manager whenever they reasonably believe that there has been a Security Incident; SCM will notify the Customer if required. This includes but is not limited to the employee notifying SCM immediately if any

computer or mobile device becomes accessible to any unauthorized party, no matter how briefly, including repairs, loss, or theft.

2. Upon demand, the employee will cooperate with SCM's or its Customer's inspection of mobile devices that access SCM or Customer systems or house SCM Confidential Information.

3. Upon 20 days' notice, the employee will cooperate with SCM's or its Customer's inspection of (a) computerized or paper systems used to share, disseminate or otherwise handle SCM Confidential Information; and (b) facilities and resources used in providing case management services (e.g., home office).

(e) Computers (including Tablets that function as Computers)

1. The employee will maintain any SCM or Customer Confidential Information solely on SCM-owned individual computers or in SCM accounts or programs provided by SCM or its Customers that permit them to remotely disable the account or program and delete its data. The employee will not place any SCM or Customer Confidential Information on any server or removable media such as an external hard drive, flash drive, SD card, or transcription device.

2. The employee will leave active at all times on the SCM-owned individual computer: encryption, current antivirus software and definitions, and all software updates affecting security.

3. The employee will comply with SCM's current policies regarding data destruction.

(f) Non-Computer Mobile Devices (e.g., Phones, Tablets) and Cloud Storage

1. The employee will not maintain any SCM Confidential Information in the internal or removable storage (such as micro SD card) of an SCM-owned mobile device or in any cloud service (such as Dropbox, Google Drive, OneDrive, or iCloud). Any Confidential Information (such as Contract-related contacts, calendar, or tasks) that appears on a mobile device will be maintained through designated accounts or programs provided by SCM or its Customers that permit them to remotely disable the account or program and delete its data.

2. The employee will leave active at all times on the SCM-owned mobile device: encryption and all operating system and application updates affecting security. When an update is proposed for the mobile device's operating system, the employee will notify SCM immediately.

3. The employee will use passwords for all devices that meet SCM's current policies, including using a different password than the device's password for any application that contains SCM Confidential Information.

(g) Disclaimer

The foregoing Confidentiality and Information Security Requirements ("Requirements") do not impose any mandatory obligations on SCM which, in its sole discretion, shall enforce, act

upon, and undertake any or all such rights and requirements on its part. SCM's failure to enforce, act, or undertake any rights or actions hereunder shall not be deemed a waiver or approval of any employee acts, omissions, performance, or otherwise, both at the time and in the future. All employee requirements hereunder are mandatory.