GINGER CARE, INC.
COMPLIANCE PROGRAM MANUAL

12-22-2023

I. INTRODUCTION 2
II. PROGRAM MONITORING RESPONSIBILITIES 4
A. CORPORATE COMPLIANCE MANAGER 4
B. COMPLIANCE COMMITTEE 5
C. DISSEMINATION OF INFORMATION 5
D. TRAINING PROGRAMS 6
E. MONITORING AND AUDITING 7
F. PRESERVATION OF DOCUMENTS 8
III. MONITORING COMPLIANCE IN SPECIFIC SUBSTANTIVE AREAS 8
A. COMMITMENT TO COMPLIANCE 9
B. COMPLIANCE WITH THE CODE OF CONDUCT 9
C. FRAUD AND ABUSE LAWS 9
D. PROPER BILLING AND PAYMENT 9
E. PROPER DOCUMENTATION 9
F. QUALITY OF CARE 10
G. RELATIONSHIPS WITH PHYSICIANS AND OTHER HEALTHCARE PROFESSIONALS/PROVIDERS 10
H. MARKETING 10
I. CONFLICTS OF INTEREST 10
J. CONFIDENTIALITY/BUSINESS INFORMATION 10
K. EMPLOYEE RIGHTS 10
L. CLIENTS' and PATIENTS' RIGHTS 10
M. DEALING WITH ACCREDITING AND LICENSING BODIES 11
IV. RESPONDING TO POSSIBLE CODE VIOLATIONS 11
A. REPORTING OF POSSIBLE VIOLATIONS 11
B. THE COMPANY'S RESPONSE 12
C. REMEDIAL ACTION 13
D. DISCIPLINE FOR VIOLATIONS 14
E. GOVERNMENT INVESTIGATION 15
V. CONCLUSION 15

I. INTRODUCTION

Ginger Care, Inc. ("the Company") and all of the communities which it operates are committed to providing their clients and patients with the level of services necessary to maintain each client's or patient's comfort and dignity while complying with all applicable federal, state and local laws and program requirements. Wingate Senior Living, LLC ("Wingate"), as Management Agent for the Company will be responsible for all of the corporate compliance functions for the Company. The Company and Wingate have instituted this Compliance Program (the "Program"), a Code of Conduct (the "Code") and other related policies to reflect these commitments. A copy of the Code is attached hereto as Attachment 1.

This Program sets forth the means by which the Company will implement the Code and related policies for its own conduct and for conduct at all of the facilities which it operates, how it will monitor compliance with the Code, and how it will respond to violations of the Code.

The Company and Wingate has designed the Program to meet the requirements of the Federal Sentencing Guidelines for organizations as a, "program that has been reasonably designed, implemented, and enforced so that it generally will be effective in preventing and detecting criminal conduct". As such, the Program includes the following elements:

(1) standards of conduct contained in the Code to assist employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents to comply with the laws pertaining to false claims, kickbacks and physician self-referrals;

(2) designation of the Compliance Manager and Compliance Committee;

(3) a system to monitor whether employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents have been sanctioned by the Medicare/Medicaid programs;

(4) education and compliance training programs for all employees executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, and agents regarding compliance and the principles articulated in the Code relevant to each such individual's role within the organization and the risk areas within which each such individual operates;

(5) a process to report violations of the Code and the adoption of procedures to protect anonymity of such reporting and to protect individuals from retaliation, retribution, or intimidation due to reporting;

(6) a system to respond to allegations of Code violations, and of procedures to enforce appropriate disciplinary action against employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents who have violated principles contained in the Code;

(7) methods to monitor compliance with the Code; and

(8) procedures to correct systemic non-compliance with the Code.

The Company entrusts its supervisory personnel with the responsibility for achieving compliance with the Code and other policies. All supervisory personnel must set an example for other employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents by conducting their duties in compliance with the Code and related policies.

Supervisory personnel are responsible for ensuring that the individuals they supervise understand their obligation to (i) comply with the standards contained in the Code and related policies, (ii) immediately report any potential violation of the Code and related policies to their supervisor or the Compliance Manager, and (iii) assist the Company in investigating any allegations of violations.

II. PROGRAM MONITORING RESPONSIBILITIES

A. CORPORATE COMPLIANCE MANAGER

Wingate has designated the person named on Attachment 2 as the Compliance Manager. The Compliance Manager will:

(1) have responsibility to oversee compliance with all applicable laws, the Code, and all related policies and procedures;

(2) have responsibility for implementing and monitoring the Program;

(3) coordinate annual updating of the Code and related policies and the Program;

(4) monitor the day to day compliance activities of the Company;

(5) oversee the Company's training of employees, executives, officers, directors, board members, and volunteers in compliance related subjects;

(6) ensure that independent contractors, vendors, and agents who are involved in the provision of client or patient services or the billing process (collectively, "Designated Contractors") are aware of the requirements of the Program;

(7) coordinate with Human Resources the pre-screening of all employees, executives, officers, directors, board members, associates, appointees, and Designated Contractors, including monitoring the National Practitioner Data Bank, the OIG's list of Excluded Individuals/Entities, and the GSA's list of debarred contractors with respect to employees, volunteers and Designated Contractors;

(8) routinely identify compliance risk areas, with the assistance and input of members of the Compliance Committee;

(9) coordinate annual internal audits of certain departments to monitor the extent to which the departments are complying with the Code;

(10) coordinate with legal counsel the internal investigation of all credible allegations of material violations of the Code;

(11) coordinate with legal counsel, management and the Compliance Committee in submitting any reports to government enforcement authorities; and

(12) report on at least a quarterly basis to the Governing Board and the Compliance Committee on: (a) progress of implementation of the Program, (b) results of on-going monitoring, including internal audits, (c) summary of regulatory changes pertaining to the fraud and abuse laws, (d) summary of proposed changes to the Code, and (e) a summary of disciplinary actions resulting from Code violations.

The designation of a Compliance Manager in no way diminishes each supervisor's responsibility to ensure that those personnel he or she supervises will comply with the Code and related policies.

B. COMPLIANCE COMMITTEE

Wingate has established a Compliance Committee, which shall evaluate and take action upon any matter that may be brought to its attention regarding the Code and the Program. The members of the Compliance Committee are listed on Attachment 3. The Compliance Committee will hold regular quarterly meetings and will hold special meetings as may be necessary. At Compliance Committee meetings, the Compliance Manager shall poll each member of the Compliance Committee to evaluate compliance in their respective areas of management. Additionally, the Compliance Manager will report to the Compliance Committee on any significant actions taken by the Compliance Manager and provide updates on any compliance related issues.

C. DISSEMINATION OF INFORMATION

In order to implement the Program, the Company will communicate the compliance requirements contained in the Code and related policies to employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents. The Compliance Manager shall establish procedures to ensure that employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents are familiar with the Code. These procedures shall include:

(1) Every newly hired employee, executive, officer, director, board member, volunteer, associate, appointee, and affiliate will receive a hard copy of the Code of Conduct Summary and other policies relevant to his/her

employment and/or engagement. Each such person will receive a hard copy of the Code of Conduct Summary during facility orientation and sign and return the certification which is attached to the Summary, confirming that they have received, read, and understand the Code of Conduct and will abide by its terms. The Code of Conduct will also be available on an ongoing basis in hard copy and online. Annually, each such person must also sign a certification in the form of Attachment 4 stating that he/she has read, understands and agrees to abide by the Code and other relevant policies. The Compliance Manager will ensure that these certifications are retained as corporate records.

(2) Additionally, upon commencement of employment with the Company and/or its Appointees, and annually thereafter, every employee, executive, officer, director, board member, independent contractor, and volunteer shall complete an online curriculum and testing in the Company's compliance policies. Participation in, and completion of, the online compliance training will be tracked online.

(3) All employees, executives, officers, directors, and board members, and volunteers will be required to attend additional in-services and/or compliance trainings regarding the Code and other policies relevant to each such individual's role within the organization and the risk areas within which each such individual operates, and to agree to comply with the Code's requirements.

(4) Upon retention, all Designated Contractors of the Company who have responsibilities related to resident care or Medicare or Medicaid billing will receive a hard-copy of the Code of Conduct Summary and will be provided access to complete copies of the Code of Conduct and Compliance Program Manual via Ginger Care's website. Upon retention, and upon each contract renewal, Designated Contractors must sign the certification form attached to the Code of Conduct Summary stating that they have read, understand, and agree to abide by the Code and Compliance Program Manual. The Compliance Manager will ensure that these certifications are retained as corporate records.

D. TRAINING PROGRAMS

The Compliance Manager will oversee and coordinate training for employees and volunteers in the principles contained in the Code and Program. Training procedures shall consist of the following:

(1) Managers and Directors will ensure that the appropriate employees and volunteers under his/her supervision receive mandatory training in the principles articulated herein, in the Code on an annual basis. The Compliance Manager and Compliance Committee will assist in the preparation and presentation of training seminars to facilitate the training.

(2) The Compliance Manager or designee will retain the attendance lists of all attendees at training sessions and copies of all training materials used.

A comprehensive education program covering compliance issues and the expectations of the compliance program will be developed by management leadership with annual participation from staff members as appropriate;

Compliance training is included in the orientation of all new employees, executives, officers, directors, board members, and volunteers;

Teaching methods will consist primarily of interactive computer-based training models, as well as video conferences or presentations, and may include other educational media as appropriate;

The Compliance Manager or designee maintains a record of dates, attendance, topics, and distributed materials;

Attendance and participation in the staff education and training program is a condition of employment; and

Failure to participate in the staff education and training program results in disciplinary action.

E. RISK ASSESSMENT, MONITORING, AND AUDITING

On an annual basis, the Compliance Manager will conduct a risk assessment and mitigation process. The Compliance Manager will use the annual OIG Work Plan as a guideline in conducting the risk assessment and mitigation process. The process will further include: (1) identification and prioritization of compliance related risks, (2) development of remediation plans in response to those risks, including internal auditing and monitoring of the identified risk areas, and (3) tracking of results to assess the effectiveness of the remediation plans. The risk assessment and mitigation process will include evaluation and identification of risks associated with the following areas: (1) submission of claims for items and services furnished to Medicare and Medicaid program beneficiaries, (2) quality of care, (3) mandatory reporting, (4) credentialing, (5) fraud and abuse laws, and (6) other risk areas as appropriate. Members of the compliance committee will participate in this risk assessment and mitigation process by evaluating and reporting on the needs of their specific departments.

The Compliance Manager will additionally oversee the Company's level of with applicable federal and state laws, regulations and programs and generally with the principles articulated in the Code.

The Company's monitoring and auditing procedures will include, at a minimum, internal and external annual audits of the company to assess levels of compliance with the Code's policies pertaining to proper billing, reporting, coding, claims development and submission, quality of care, credentialing, mandatory reporting, fraud and abuse laws, and other risk areas as appropriate. If any audit reveals possible non-compliance with the Code, then the Compliance

Manager will consult with legal counsel. The Compliance Manager will take appropriate remedial action as described herein. In the event of repeated violations, The Company may consult with an external auditor.

In addition, the Compliance Manager will coordinate with Human Resources to ensure that the National Practitioner Data Bank, the OIG's list of Excluded Individuals/Entities (www.oig.hhs.gov), and the GSA's list of debarred contractors are checked with respect to all medical staff members. If Human Resources discovers that a practitioner has been sanctioned, then Human Resources will notify the Compliance Manager, who in turn will consult with legal counsel to determine whether disciplinary action should be taken against the medical staff member. In addition, prior to hiring or engaging an employee or designated contractor, the Company will conduct a CORI check as well as review the Cumulative Sanction Report to determine whether such person has been sanctioned. If the person has been sanctioned, the Company will contact the Compliance Manager, who will determine, in consultation with legal counsel, whether it is appropriate to hire or engage the person.

F. PRESERVATION OF DOCUMENTS

The Company has instituted a document retention policy with which each employee, volunteer and each designated contractor of the Company must comply. This policy appears in Attachment 5. Document retention and destruction must take place in accordance with this established, written policy. Each supervisor shall monitor compliance with this policy within his or her department.

The Compliance Manager will establish procedures to prevent the intentional or inadvertent destruction of documents that are relevant to known government investigations.

The Company must retain all potentially responsive documents if it has been served with a government subpoena or any other document request from the government (collectively, "document request"). If the Company has a strong basis to believe that there is an impending government investigation of it, the Company must retain all documents that it knows may pertain to that investigation.

If the government serves any type of document request on the Company or if the Company has reason to believe a document request may be served, the Compliance Manager is responsible for immediately directing personnel to retain all documents that may be potentially responsive to the document request.

III. MONITORING COMPLIANCE IN SPECIFIC SUBSTANTIVE AREAS

The Code applies to all employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, and agents. Each such person is personally responsible for his or her conduct in complying with the Code. Each supervisor will distribute the Code to every appropriate employee, volunteers and designated contractor whom she/he supervises. In addition to policies concerning fraud and abuse and the adherence by all employees to the commitment and mission of the Company to comply with such laws, the Code focuses on employee and volunteer conduct with respect to the laws that

most frequently and directly impact the business conduct of employees and volunteers. A brief description of the policies discussed in the Code is set forth below.

A. COMMITMENT TO COMPLIANCE

The Company's commitment to compliance is set forth in Section 1 of the Code. All employees, volunteers, independent contractors and agents are required to govern themselves in a manner that adheres to and promotes both the letter and spirit of that commitment. Adherence to that commitment shall be an element of each employee's and volunteer's annual evaluation for purposes of promotion and compensation.

B. COMPLIANCE WITH THE CODE OF CONDUCT

The Company' policies regarding compliance with laws, regulations and program requirements as well as appropriate disciplinary action for failure to comply with the Code, are set forth in Section 2 of the Code. All employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, or agents of Ginger Care will be subject to disciplinary action for engaging in – and from encouraging, directing, facilitating, or permitting any other person to engage in – any non-compliant behavior.

C. FRAUD AND ABUSE LAWS

The Company's policies regarding fraud and abuse are set forth in Section 3 of the Code. Such policies provide that all employees and volunteers understand the Company's policies with respect to false claims, kickbacks and physician self-referrals. In addition, the Compliance Manager will modify, as necessary, the Program in light of any OIG Special Fraud Alerts or other notice alerting the healthcare community to significant changes or clarifications in the fraud and abuse laws.

D. PROPER BILLING AND REIMBURSEMENT

The Company's policies regarding proper billing and reimbursement practices are set forth in Section 4 of the Code. These should guide the preparation of all claims, cost reports and other billing documents.

E. PROPER DOCUMENTATION

The Company's policies regarding the proper documentation of services are set forth in Section 5 of the Code. These policies should guide employees so that the Company only submits claims when they are based on appropriate documentation and comply with all payor billing requirements.

F. QUALITY OF CARE

Section 6 of the Code discusses the Company's commitment to providing each patient with the level of care necessary to attain or maintain each patient's care, comfort & dignity at end of life and a commitment to complying with the Medicare, Medicaid or other third party payors conditions of participation.

G. RELATIONSHIPS WITH PHYSICIANS AND OTHER HEALTHCARE PROFESSIONAL AND PROVIDERS/SUPPLIERS

The Company' policies regarding relationships with physicians and other healthcare professionals and providers/suppliers are set forth in Section 7 of the Code. These policies will help ensure that all contracts and relationships do not violate federal and state laws regarding kickbacks and physician referrals.

The Company will only enter into agreements or compensation arrangements with any actual or potential referral source that have been approved by Senior Management. The Compliance Manager is responsible for making sure that The Company complies with this procedure.

H. MARKETING

Section 8 of the Code contains the Company's Marketing policy, which requires all communications to be truthful and accurate.

I. CONFLICTS OF INTEREST

The Company's policies regarding conflicts of interest are set forth in Section 9 of the Code. These policies will guide employees, executives, officers, directors, board members, volunteers, independent contractors, agents, associates, appointees, affiliates, and others on how to avoid any conflicts between personal interests and the interests of the Company.

J. CONFIDENTIALITY/BUSINESS INFORMATION

The Company's policies regarding confidentiality of business and patient information are set forth in Section 10 of the Code. The Compliance Manager will direct program directors and supervisors to make certain that personnel in their departments understand such policies with respect to the disclosure to unauthorized persons of confidential business information including trade secrets, commercially sensitive information, and financial information about the Company.

K. EMPLOYEE RIGHTS

The Company's policies providing employees the right to a working environment free from harassment, illegal drugs, alcohol and unlawful discrimination are set forth in Section 11 of the Code. In addition to the policies discussed in Section 11 of the Code, the Company has employee policies to ensure compliance with federal laws governing employment and the workplace.

L. PATIENT RIGHTS

The Company's policies regarding patients' rights are set forth in Section 12 of the Code. Program directors shall make certain that all employees and volunteers under their supervision are aware of state and federal laws and facility licensing requirements concerning all patients' rights.

M. DEALING WITH ACCREDITING AND LICENSING BODIES

The Company's policies regarding appropriately interacting with accrediting and licensing bodies are set forth in Section 13 of the Code.

IV. RESPONDING TO POSSIBLE CODE VIOLATIONS

A. REPORTING OF POSSIBLE VIOLATIONS

The Company encourages and allows employees executives, officers, directors, board members, and volunteers to seek and receive prompt guidance before engaging in conduct that may implicate the Code or related policies. Every employee executive, officer, director, board member, and volunteer has a responsibility to report any violation of the Code or related policies to his or her supervisor or the Compliance Officer. All supervisors must report any potential violation of the Code to the Compliance Officer.

To achieve these objectives, the Compliance Manager will publicize the following practices and procedures to all employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents:

(1) Employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, and agents may consult their supervisors or the Compliance Manager about any questions regarding the Code or related policies. The supervisor should respond to any inquiry and/or refer the question to the appropriate personnel within the Company.

(2) Employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, and agents will report to their supervisors or the Compliance Manager any potential non-compliant activity, including potential violations of the Code or related policies. Supervisors who receive such reports shall report the information to the Compliance Officer. Employees, volunteers, independent contractors, associates, appointees, affiliates, and agents may not be subject to any intimidation, retaliation, or retribution for reporting, investigating, evaluating, or auditing, in good faith, a suspected violation of the Code or related policy or for their good faith participation in any other aspects of The Company's Compliance Program. Employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, and agents may report possible violations anonymously to their supervisors and/or the Compliance Officer. Except as required by law, The Company will maintain the confidentiality of the identity of such individuals who submit reports of possible violations of the Code.

(3) The Compliance Manager will establish and publicize an Anonymous Reporting Hotline for reporting possible compliance and ethics violations of the Code or related policies to the Compliance Officer. The purpose of

this service is to ensure that any employee wishing to submit a report can do so anonymously and without fear of retaliation. The Hotline will also be available for posing questions regarding the requirements of the Code or related policies. Persons accessing the Hotline may be asked to leave a message for the Compliance Manager, who will ensure that each call is returned promptly if call back information is provided. The Compliance Manager will maintain a log of Hotline calls, including the nature of any investigation and the result.

(4) All management personnel will have an "open door policy," that permits employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, and agents to present any suspected violation of the Code or related policies.

(5) The Company maintains a firm non-retribution policy and will not retaliate against any individuals who raise or report potential non-compliant activity.

B. COMPANY RESPONSE AND INVESTIGATION

The Compliance Manager shall review and investigate all reports of potential non-compliant activity, including violations of the Code or related policies, using appropriate resources. In conducting such investigation, the Compliance Manager will consult with that member of the Compliance Committee within whose area the potential violation falls and will utilize the Company's Risk Management department protocols. The Compliance Manager shall complete the initial investigation within two business days of receiving a report of a potential violation (unless additional time is necessary to complete a thorough and accurate investigation). If the Compliance Manager concludes that a violation has occurred, then within two business days of reaching such conclusion, the Compliance Manager will report the violation to the CEO with a recommendation for remedial action in order to reduce the potential for recurrence (as further specified in Sections IV(C) and IV(D) below and Section 2 of the Code of Conduct). Additionally, the Compliance Manager will ensure timely reporting, as required, to the appropriate state and/or federal agencies, including without limitation the Federal Office of the Inspector General, the New York State Department of Public Health, and the New York State Office of Medicaid Inspector General, as appropriate. The foregoing process will be appropriately tailored to meet the specific circumstances and needs of each reported violation.

All Company employees, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates and agents must cooperate fully with any internal investigation.

C. REMEDIAL ACTION

If the Company determines – through internal investigation, self-evaluations, or audits – that a violation of the Code has occurred, the Company will take prompt and thorough remedial action.

In determining the appropriate remedial action, the Company shall consider:

(1) the extent to which any person knowingly, intentionally or with reckless disregard or deliberate indifference acted contrary to Medicare or Medicaid laws, regulations or program requirements;

(2) the nature and extent of potential civil or criminal liability of individuals or the Facility;

(3) the nature and extent of a resulting government overpayment, if any;

(4) the impact the problem or incident had on the quality of services provided to clients or patients;

(5) the root cause of the violation; and

(6) the extent to which the problem or incident reflects a systemic or departmental failure to comply with the Code.

After consideration of these factors, the Company will determine the appropriate remedial action and/or discipline, which may require the Company to take one or more of the following steps:

(1) Correct the practices within the department or unit which led to the violation as soon as possible;

(2) Initiate appropriate disciplinary action against the employee, executives, officers, directors, board members, volunteer, independent contractor, associate, appointee, or agent, if any, involved in the violation, in accordance with Section IV(D), below. Such disciplinary action shall include, at a minimum, a written warning that shall be placed in the individual's personnel file and may include further discipline, up to and including termination;

(3) Undertake a program of education within the appropriate department or unit to prevent similar violations in the future;

(4) If there is a possibility that the Company received an overpayment, calculate the amount and repay the appropriate government entity or insurer; and

(5) If there is a possibility that criminal conduct has occurred, suspend all billing related to the violation in the department or unit where the problem exists until the problem is corrected, and notify appropriate government authorities.

If the investigation reveals that there is systemic non-compliance with the requirements contained in the Code, the Compliance Manager will consult with legal counsel and/or an external auditor, the Compliance Committee and the Compliance Working Committee to

evaluate (a) what form of corrective action the Company should take, if any, and (b) whether the Company should modify the Code and/or the Program to address such non-compliance.

D. DISCIPLINE FOR VIOLATIONS

The Company will document all reasons for disciplinary actions taken against its personnel for violations of the Code and related policies. The determination of the appropriate discipline shall be made in accordance with the Company's Personnel Policies and Procedures Handbook, but will include, at a minimum, a written warning, and may include one or more of the following: suspension, privilege revocation or termination. All discipline for violations of the Code shall be firmly and fairly enforced. The following factors may be taken into account in determining the appropriate disciplinary action to impose for a violation of the Code or related policies:

(1) the nature of the violation and the ramifications of the violation to the Company;

(2) the disciplinary action imposed for similar violations;

(3) any history of past violations;

(4) whether the violation was willful or unintentional;

(5) whether the individual was directly or indirectly involved in the violation;

(6) whether the violation represented an isolated occurrence or a pattern of conduct;

(7) if the violation consisted of the failure to supervise another individual who violated the Code or related policies, the extent to which the circumstances reflect lack of diligence;

(8) if the violation consisted of retaliation against another individual for reporting a violation or cooperating with an investigation, the nature of such retaliation;

(9) whether the individual in question reported the violation; and

(10) the degree to which the individual cooperated with the investigation.

E. GOVERNMENT INVESTIGATION

If the need arises, it may be appropriate to inform the Company personnel that the government is conducting an investigation of certain matters and that government investigators may contact employees in connection with the investigation. If such an investigation is to occur, the Compliance Manager may inform employees, executives, officers, directors, board members, volunteers, independent contractors, associates, appointees, affiliates, and agents of their rights and obligations with respect to requests for interviews from governmental investigators, which

information shall conform to the policy stated in Attachment 6. Employees, executives, officers, directors, board members, and volunteers should refer any contact from a government official regarding an investigation to the Compliance Manager and report such contact to the Compliance Manager.

V. CONCLUSION

The Compliance Manager and Compliance Committee will review this Program and the Code annually to assess whether it reflects the appropriate principles to facilitate the Company's compliance with all federal and state fraud and abuse laws and sound ethical business practices. If you have suggestions for additions or other changes to the Program or the Code, contact the Compliance Manager.

ATTACHMENT 1

CODE OF CONDUCT
POLICY MANUAL

ATTACHMENT 2

DESIGNATED COMPLIANCE OFFICER

The Compliance Manager for the Company is:

Maureen S. Brinn
Chief Compliance Officer
Wingate Living.
57 Wells Avenue
Newton, MA 02459

Phone: 781-707-9085
Cell: 617-777-4474
eFax: 781-707-9085
Email: mbrinn@wingateliving.com

Anonymous Reporting Hotline: 1-877-860-7355 Available 24 hours/day, 7 days/week

ATTACHMENT 3

MEMBERS OF COMPLIANCE COMMITTEE

The Members of the Compliance Committee for the Company are:

Chief Compliance Manager
General Counsel
Chief Financial Officer
Chief Operating Officer
Vice President of Clinical Services
Senior Systems Engineer
Director of Clinical Reimbursement
Director of Payroll & Benefits

ATTACHMENT 4

CERTIFICATION FORM

EMPLOYEE CERTIFICATION AND AGREEMENT OF COMPLIANCE

I certify that I have received and read the **Ginger Care, Inc. Code of Conduct** (the "Code") as an integral part of my compliance training and will retain a copy of the Code for my guidance. I fully understand the requirements set forth in the Code. I agree specifically to act in accordance with the policies set forth in the Code and understand that failure to report violations to my supervisor or to the Company's Corporate Compliance Manager may be grounds for sanctions, ranging from reprimand to termination. I will forward an original signed copy of this affirmation statement to my immediate supervisor.

I also understand that the Code does not represent any type of employee agreement or contract and that my employment is on an "at-will" basis as further explained in the Company Employee Handbook. The Company may, at any time, unilaterally modify and amend the policies and/or requirements contained in the Code.

Dated: _____

_____
Signature

_____
Printed name

ATTACHMENT 5

DOCUMENT RETENTION POLICY
Rev. 8/8/2022

I. INTRODUCTION

Each employee of Ginger Care, Inc. (the "Company") must adhere to the requirements set forth in this Document Retention Policy. Each employee is personally responsible for his or her own conduct in complying with this Policy. Employees must cooperate with the Compliance Manager who shall be responsible for administering and monitoring the Document Retention Policy.

- The Company has established specific retention requirements for certain categories of documents. For specific retention periods, please see the Record Retention Schedule at the end of this policy. No destruction should occur if it could otherwise be construed as an obstruction of justice or violation of law. Any questions in this regard should be raised with the Compliance Manager before documents are destroyed.

- If there is reason to believe that a violation of the Document Retention Policy has been committed or that a government investigation exists or is imminent, no relevant documents should be destroyed until clearance has been obtained from the Compliance Manager.

- Responsible employees shall retain indefinitely all acknowledgments and certifications signed by the Compliance Manager as required by the record destruction policy which follows.

II. POLICIES AND PROCEDURES

a) Purpose:

The Company has adopted this Document Retention Policy to ensure that records are retained for a uniform time period by employees and to avoid the unnecessary accumulation of documents. The purposes of the Document Retention Policy are:

- to meet current needs in record storage and retrieval systems;
- to ensure compliance with various governmental regulations concerning document retention periods;
- to promote the cost-effective management of records;
- to update any previously issued record retention schedules;
- to maintain documentation consistent with the Company's Corporate Compliance Program; and
- to ensure uniformity in records retention.

The Policies and Procedures set forth herein apply to all documents and records maintained in paper or electronic form, including without limitation computer storage, microfilm, microfiche,

disks, tapes, and electronic mail ("e-mail"). The terms "records" and "documents" are interchangeable and include originals and copies of all correspondence, contracts, charts, ledgers, forms, books, drawings, photographs, film, video, sound records, or any other materials used in business operations.

b) Compliance Manager

The Compliance Manager will be designated and have ultimate responsibility for overseeing compliance with this Document Retention Policy. The Compliance Manager will be empowered to appoint other or supervisory personnel to assist in this oversight. The essential function of the Compliance Manager is to ensure that a chain of responsibility is in place for coordinating and implementing this Document Retention Policy. The Compliance Manager and other supervisory or the Company Compliance Committee appointees shall seek the assistance and guidance of legal counsel whenever needed to answer any questions regarding this Document Retention Policy. The designation of a Compliance Manager or any appointees thereof in no way diminishes the responsibility of each employee to comply with this Document Retention Policy.

c) Retention Periods

Records shall not be destroyed before the period prescribed in the Record Retention Schedule has expired. Retention periods should apply only to original documents unless otherwise specified. Duplicates should generally be discarded after use unless necessary to support current operations. If duplicates are so retained, they should be discarded after they have served their purpose.

In no event should any document be retained for a period longer than the retention period of the original document without first contacting the Compliance Manager or appointed supervisor. Physicians, employees should not selectively discard records or other documents that would normally be retained for a longer period of time because they believe that the documents might be harmful to any employee or to the Company**.**

Record retention periods are generally based on federal and state statutes and regulations, or are as long as the statute of limitations for filing a suit which is based upon that record. In cases where both federal and state laws may apply, the longer of the two periods is applied. For some classes of documents, there are no legally mandated retention periods and those prescribed in the Record Retention Schedule are based on customary business practice and reasonable necessity. For records not listed on the Record Retention Schedule, employees should consult the Compliance Manager to determine the length of the retention period.

d) Records Destruction Policy

When records are destroyed in an organized fashion, based upon a written policy or regular schedule, there may be an effect on any investigation or litigation. Destruction of records without such procedures may be seen as suspect in the event of an investigation or litigation. The most common record destruction schedule is once a year in a specified month. The following principles should be adhered to:

- No records should be destroyed in any manner inconsistent with this Document Retention Policy, including the Record Retention Schedule, or in any manner inconsistent with the direction of the Compliance Manager;
- Prior to destruction, documents should be classified, and a random sample of each category should be examined for content and scope (a full inventory is generally not necessary).
- Destruction should be pursuant to a designated plan.
- Destruction of electronic records should involve down-loading them to an off-line storage media such as a magnetic tape or diskette, followed by erasure or deletion.
- All records should be destroyed during the same time period.
- A permanent record should be kept to document the scope of documents destroyed, the date of destruction, and the identity and signature of the Compliance Manager or person supervising the record destruction.
- If a professional record destruction company is used, the contract should clearly define the procedures to be followed and provide for a method to safeguard the confidentiality of any of the records.

A one-time destruction program to initially eliminate records consistent with this Document Retention Policy may be permitted if performed pursuant to the procedures outlined above and consistent with the direction of the Compliance Manager.

If the Company receives a subpoena or is involved in or aware of any pending or imminent investigation, proceeding or civil action to which its records are relevant, no records potentially relevant to such matters should be destroyed even if destruction is indicated under the document destruction policy. Under these circumstances, destruction of records could subject the Company to prosecution for obstruction of justice or contempt of court.

e) Records Relevant to More than One Category.

When records may be subject to more than one category listed in the Record Retention Schedule, employees must use the longest retention period. Employees should never guess as to the retention period applicable to a particular record or category of records. Any questions in this regard should be directed to the Compliance Manager.

f) Copies.

Only one copy of each record must be retained to comply with record retention requirements. Participants in a project should make efforts to arrange for only one common file of project documents to be maintained. All duplicates of documents should be destroyed when no longer necessary.

g) Electronic Records.

Electronic records should be filed, labeled and retained in the same manner as paper records so as to permit review and a determination of the applicable retention period. E-mail should also

be treated similarly to paper records (i.e., e-mail messages which are generated daily when working on a matter--analogous to information found on Post-It Notes--may be deleted; however, e-mail that is important and related to a particular project should be filed and retained). Employees may opt to print such messages and retain them in hard copy.

h) Emails

The Company will retain all emails for three (3) years. After three years, all emails will be automatically scheduled for deletion, except as follows:

Emails related to potential or active litigation will be marked for retention, until further instructed by Legal. Emails to be retained for potential or active litigation will include (a) any emails containing the name of a GL/PL claimant which are in the custody of any employee of the facility in which such resident resided or which are in the custody of any home office employee, and (b) any other emails identified by the Legal Department related to any other potential or active litigation.

i) Exceptions.

Any exceptions to the Company's Document Retention Policy should be made only after consultation with the Compliance Manager. Any employee or volunteer who believes that circumstances warrant such a deviation should promptly contact the Compliance Manager.

j) Investigations, Legal and Administrative Proceedings.

Notwithstanding any provision to the contrary in this policy or retention period listed in the Record Retention Schedule, all document destruction procedures shall immediately be held in abeyance in the following circumstances:

- The records may be covered by a subpoena that has been issued (or other existing request) or there is reason to believe that the records may be subpoenaed (or otherwise requested) in a current or impending matter;
- There is an existing or impending internal or governmental investigation, civil litigation or other legal or administrative proceeding that may reasonably require production of the records; or
- The Company is voluntarily cooperating with the governmental authorities or other outside parties in a legal or administrative proceeding that may reasonably require production of the records.

The Compliance Manager has the primary responsibility of promptly notifying appropriate employees of the occurrence of any of the above events to ensure that a proper "HOLD" is placed on record destruction. Generally, specific instructions regarding the "HOLD" will be appropriately disseminated. If there is any question whether a particular document is, or should be, subject to a "HOLD" designation, the Compliance Manager’s approval must be obtained prior to the destruction of such documents.

Any employee who has reason to believe that the above-described or any other circumstances warrant retention of the Company’s records beyond the required periods should

preserve the records in question and immediately contact the Compliance Manager.

k) Privileged and Otherwise Protected Documents.

The Company is entitled by law to keep certain documents confidential, even when sought by an opposing party in a legal proceeding. Such documents are commonly referred to as privileged. The Company's policy is to maintain the confidentiality of privileged documents.

There are several types of protection against disclosure, including the attorney-client privilege, the work product doctrine and, in some circumstances, the self-evaluation privilege. The attorney-client privilege applies to confidential communications between a client (the Company) and its attorneys (lawyers retained to represent the Company). The work product doctrine protects documents prepared in connection with, or in anticipation of, litigation that reflect legal strategies and attorney thought processes. Documents of a sensitive or confidential nature such as business plans, trade secrets or strategic plans warrant special attention to preserve confidentiality and unnecessary duplication.

Other privileges may apply to a resident's clinical record, including but not limited to the social worker-client privilege or the psychotherapy privilege. These privileges apply to communications between certain providers and residents. Documents containing these types of records also warrant special attention to preserve privilege.

In order to maintain the privileged nature of a document, the rules defining the privilege must be strictly observed. One rule common to all privileges is that the privileged document must be kept confidential from third parties. If an otherwise privileged document is shared with a third party, the privilege might be lost forever. If any employee is a custodian of documents that might be privileged, that individual should (i) notify the Compliance Manager, and (ii) ensure that the documents are segregated in files and marked "privileged and confidential."

l) Work Files.

Personal work files may be maintained so long as a matter is pending. Once a matter is concluded, records contained in a work file should be categorized and retained or discarded in accordance with the prescribed retention periods. Personal copies and informational copies kept by physicians and employees have the same force as an "original" copy in a court of law. Thus, these records may be subpoenaed from an employee, even if the original has been destroyed.

III. CONCLUSION

The Company is committed to strict compliance with all laws and ethical standards by all of its employees. Any questions regarding issues raised by this Document Retention Policy should be directed to the Compliance Manager or the Company's attorneys.

RECORD RETENTION SCHEDULE

	Records	Retention Period
MEDICAL RECORDS	Medical Records	10 years
	Med Record Destruction certificate	Permanent
	Credentialing Files	10 years
MINUTES	QA/PI Minutes	10 years
	Safety Minutes	4 years
	Environmental Rounds	10 years
	Resident/family council meeting	10 years
MISC	SDS Sheets (Safety Data Sheets)	30 years
	Certificate of Insurance	4 years
	Contracts; post termination	6 years, or 20 years if under seal
	Visitor Logs	3 years
	Admission/Discharge logs	5 years following cost report
	Medical, Bio Waste Disposal	375 days after material is disposed
	Hazardous Waste Transport and Dispos.	See Medical, Bio Waste Disposal Records
	Emails	3 Years. Emails related to potential or active litigation will be marked for retention, until further instructed by Legal.
	Daily Census Summary	5 years following cost report
	Fire/Emergency Drill Reports	5 years
NURSING DOCUMENTS	Narcotic Books	10 years
	Controlled Substance Destruction (See Narcotic Books)	
	Infection Control Summary Reports	10 years
	Infection Control (Other) (See Infection Control Summary Reports)	
	Nursing Assistant Assignment Sheet	2 years
	Incident Reports	10 years
	Supervisor Report Sheets	2 years

	24 hour report sheets	2 years
	Resident Concerns/Grievances	10 years
	Alarm Logs	2 years
	Accreditation Survey and Reports	3 years
	Wanderguard Testing Sheets	4 years
	Posted Daily Staffing Sheets	10 years
WORKSHEETS	Weight Sheets/logs	See medical records
	Dining Room Intake	See medical records
	24 hour reports	See medical records
	Nursing Report/Communication Books	See medical records
	Assignment Sheets/daily staffing	See Nursing Assistant Assignment Sheets and Posted Daily Staffing Sheets
	Pressure Ulcer Logs	See medical records
	Safety Observation Sheets	See medical records
HUMAN RESOURCES	Employee files	5 years
	I9 Forms	5 years
	Benefits	5 years
	Payroll	5 years
	Medical	30 years following employment
	Background checks	See employee files, except Criminal Offender Record Information, which must be maintained for a minimum of 3 years but cannot be maintained for more than 7 years.
	Applications	See Employee Files
	OSHA Logs	5 years following the end of the year to which they relate
	Employee exposure records	30 years
	Employee injury reports	5 years following the end of the year to which they relate
ACCOUNTS RECEIVABLE	UB04's	6 years
	Month End Invoices from Vendors & AP Vouchers	6 years
	Rehab Logs	7 years
	Ancillary charge efiles e.g. Therapy & Pharmacy	6 years

	Resident Financial documents	6 years
	Admission Agreement	10 years
	State & Federal Audit Records & supporting documentation	10 years
	Payer Audit Records & supporting documentation	10 years
	Rate Letters	Until cost report is settled
	Processed Refund Requests including copy of checks	10 years
	Rug Score Billing Change Logs from MDS	10 years
	Census change documents	5 years from date of cost report

ATTACHMENT 6

RESPONDING TO GOVERNMENT INVESTIGATIONS

GUIDANCE TO EMPLOYEES AND VOLUNTEERS WHO ARE CONTACTED BY GOVERNMENT OR PRIVATE INVESTIGATORS

I. INTRODUCTION

At some point during your employment or volunteer work with the Company, an employee of the federal or state government, or of a private insurer, may contact you as part of an investigation. The purpose of this document is to provide you with advice on how to respond to such contact and to ensure:

(1) That all communications from the Company and its employees, volunteers and contractors to any government or private investigator are truthful and accurate.

(2) That the legal rights and privileges of the Company and all of its employees, volunteers, clients and contractors are protected and that all persons have the opportunity to choose whether or not to exercise their rights to the full extent allowed by the law.

If at any time a person contacts you and claims that he[1] represents any investigative agency, you should follow the procedures outlined in this document. In addition, if any investigator contacts you, you should contact the Company's General Counsel at 781-707-9000. If the General Counsel is not available, call any one of the Compliance Committee members indicated in Attachment 3. Please feel free to call collect or, if you choose to call directly, the Company will reimburse you for any long distance charges.

It is the Company's policy to cooperate with government investigations in the most accurate and truthful manner possible. However, in order to ensure that such cooperation occurs in an organized and accurate manner, it is important that the Company conduct such communications through its Compliance Manager and legal counsel.

Furthermore, though the decision to speak with any government representative is your decision to make, you do not have the authority to provide any outside person with the Company's property or access to the Company's real property. Therefore, you do not have the authority to give any documents, computer systems, or other tangible objects and stored information that are the Company's property or the property of its clients, to any person, including a government investigator. All such documents will be produced through the Compliance Manager and the Company's legal counsel. You do not have the authority to allow any investigator into the Company's offices or its clients' offices. Any person requesting any such documents, information, or access, should be immediately directed to the Compliance Manager or legal counsel. The only

exceptions to this are law enforcement officials who present a valid search warrant. The procedure for a search warrant is described below.

II. WHO MAY CONTACT YOU?

There are a variety of federal and state agencies involved in healthcare enforcement. In addition, private insurance companies, Medicare intermediaries and carriers, and others have investigative offices. Among the agencies that may contact you as part of an investigation are:

(1) Federal Bureau of Investigation,

(2) Office of Inspector General ("OIG") of the Department of Health and Human Services,

(3) U.S. Attorney and the Department of Justice,

(4) State Attorney-General,

(5) Medicaid Fraud Control Unit of a State Prosecutor's Office,

(6) Internal Revenue Service,

(7) U.S. Postal Inspectors,

(8) Medicare Intermediary and Carrier, and

(9) State Boards that oversee Doctors, Chiropractors, Nurses, etc.

If you are contacted by any person who claims to be acting in an official capacity as part of an investigation or government action, and you are not sure whether or not this person is a duly authorized investigator, immediately contact your supervisor, the Compliance Manager, or the Company's legal counsel as discussed above.

Please keep in mind that a government investigator does not necessarily have to identify himself and present his credentials before asking questions or seeking documents or authorization to inspect any physical premises. If a person makes any such inquiry, please question him as to his authority and nature of his business before providing any answers. Investigators may use an assumed or false identity when seeking information and the law does not require them to accurately identify themselves. Business competitors or other persons may also make such inquiries, and you should not provide any information to such persons. If you have any concerns about the status of the person making any such inquiries or are concerned about the nature of such inquiries, immediately contact your supervisor, the Compliance Manager, or the Company's legal counsel.

III. RESPONDING TO REQUESTS FOR INTERVIEWS

An investigator may contact you in a variety of settings, including your office, at a client's office, or at home. Regardless of the place of contact, you should respond in the same manner:

(1) Confirm the Investigator's Identification. If the investigator has contacted you in person, ask to see his identification and business card. Make sure you write down his name, title, address and telephone number. You should immediately call his office to confirm his authority before having any further contact with him.

If the investigator contacts you by telephone, ask him for his name, title, office address, and telephone number, and the general purpose of the call. Before having any discussion with him you may want to confirm the authenticity of the investigator's credentials through the Company's legal counsel or the Company's Compliance Manager. Therefore, you may not want to discuss anything in the initial telephone contact but return the call at a later point once this confirmation takes place.

(2) Your Right to Consult With a Lawyer. Whether or not you speak with a representative of the government is your own individual decision to make. You may speak with him, refuse to speak with him, or delay any decision until you have received the advice of legal counsel. the Company will provide you with legal advice from its own attorney, or, as appropriate, an attorney retained specially to represent you. We strongly recommend that you do not make any decisions concerning your legal rights until you have had the opportunity to consult with legal counsel. Whatever you choose to do, it is important that any information you give is accurate and truthful, to the extent you choose to discuss anything.

Whether you consent to an interview, and the choice of the date, time and location of that interview, are for you to decide. You have the right to consult with legal counsel before giving a response to any government investigator requesting an interview. If any investigator suggests that you have to speak with him, that you should not consult with legal counsel, or that you should feel guilty if you do not immediately consent to an interview, this is improper and unethical. You should not feel intimidated by such statements nor should you feel any pressure to submit to such a suggestion. The law does not require any person to speak with an investigator on the spot. It is entirely appropriate for you to inform him that you will get back in touch with him at a later date. This will enable you to consult with legal counsel and to make your own decision upon appropriate reflection. You need only say that your lawyer or the Company's lawyer will get back in touch with the agent and you may terminate the interview immediately, if you so choose.

(3) Attorney May Attend Interview. During any interview that you agree to cooperate with, you have the right to have an attorney present. The Company will arrange to have the appropriate attorney or supervisor present and to meet with you beforehand at no cost to you. You may of course consult with an attorney of your own choosing at your own expense at any time in addition to or instead of consulting with the attorney supplied by the Company.

(4) Immunity and Promises. An agent or investigator cannot make a binding promise on behalf of the government. A suggestion by any agent or investigator that he will go easy on you, that speaking to him will help you, or that he can give you any kind of immunity or protection from legal consequences is not accurate. Only a prosecutor employed by the government can make such commitment and it is proper and expected that such commitments are made in writing, not orally.

(5) Take Notes and Inform the Compliance Officer. If you choose to speak with the government investigator, we request that you contact the Compliance Manager or the Company's legal counsel immediately after the interview. You have every right to take detailed notes during any such interview and to share the contents of those notes with the Company's legal counsel. Any statement by the government investigator that it is improper or that discourages you from taking notes, or sharing those notes with the Company's legal counsel, is improper and

you should not submit to such pressures. You do not have to share your notes with any person including government investigators.

(6) Always Tell the Truth. If you choose to speak to an investigator, always remember that you should speak only in a truthful and accurate way. You should not intentionally or negligently misrepresent any fact, no matter how trivial you may think it is or how embarrassing it is to you. Though you have the right to choose not to respond, you do not have the right to provide misleading or false information. If you do not have sufficient information to provide a full or accurate response, you should inform the government representative of this and you may tell him that you will discuss the subject with him at a later point. You should never guess or speculate merely to provide an answer. If you do not have full information, you should not be embarrassed about saying so. Nor should you ever pretend that your information is based upon first-hand knowledge when it is not. If you witnessed something, heard something directly or saw it, you should so indicate. If you know something only because it was repeated to you by another person, or you have surmised it, you should not represent this to be knowledge based upon first-hand experience.

(7) If the government sends you a subpoena or any document in the mail requesting documents or information that is the property of the Company or one of its clients, immediately give it to the Compliance Manager or the Company's legal counsel. Do not respond to any such request until receiving instructions from one of them.

IV. SEARCHES

Frequently an investigator will ask for an opportunity to search the premises or to obtain documents or tangible objects from the premises. Under no circumstances should you interfere with a legally authorized search warrant. However, please keep in mind:

(1) Any time a government representative looks inside a closed container (i.e., mail, package, luggage, automobile, etc.) or enters any physical premises to inspect the premises, or to look for objects, this is considered a search. If the investigator requests permission to search any Company facility or property or to receive documents or other tangible objects, you have no authority to give him permission. Refer him to the Compliance Manager or the Company's legal counsel immediately. You are not authorized to grant an investigator permission to search any Company facility or property, or to give him any tangible object.

(2) Generally, a government representative can only conduct a search if he has a legally valid search warrant. The only exception to this is under certain circumstances Medicare and Medicaid providers are required to grant government agencies and carriers immediate access to records or premises. Such agencies include the Office of the Inspector General of the Department of Health and Human Services, the state Medicaid Fraud Control Unit, and the Medicare Carrier and Intermediary. If such entities request an opportunity to inspect records under such authority, you should cooperate and do so in a courteous and respectful manner. When responding to their request, you should ask for sufficient time to contact the Compliance Manager or the Company's legal counsel, and have them speak with the requesting person and make the arrangements to respond to the request.

(3) If the government representative presents you with a search warrant, you should immediately contact the Compliance Manager, legal counsel, or your supervisor for

assistance in determining whether or not the warrant is valid. The warrant can only legally authorize a search if it is signed by a federal or state judicial officer and authorizes the search of identified premises during a particular date and time. If the government investigator presents you with a copy of a search warrant, read it before authorizing his entry. Make sure it correctly identifies the address and description of the premises to be searched, and that it gives the appropriate date and time for the search. The government is not allowed to conduct a search on a date or time that is different from the date and time period specified in the search warrant. If the warrant does not correctly identify the address, premises, date or time, you may point that out to the investigator and politely ask if it is still appropriate to conduct the search.

(4) If the investigator presents you with a copy of a duly authorized search warrant, confirm the investigator's identity and allow him to execute the search warrant. Retain a copy of the warrant. Ask for a copy of the affidavit supporting the warrant, but remember, the investigator is not required to give you this affidavit.

(5) A warrant authorizes the government to conduct a search, but it does not require people to respond to any requests for interviews. Most importantly, it does not reduce or undercut in any way your right to consult with legal counsel before deciding to respond to any request for an interview or for cooperation. Though you have no obligation to participate in any interviews under the warrant, you cannot take any steps to obstruct the government's search. At no time should you interfere with the search in any way. You should not provide investigators with false information. You should not destroy, hide or alter any documents or objects.

(6) You have the right to observe the search during the execution of the search warrant, so long as you do not interfere with such execution. You have the right to take detailed notes on what you observe the government investigators doing. You may videotape or photograph the search if such equipment is available. You do not need to share your notes, photographs or videotape with the agents conducting the search.

(7) If the government is looking to remove documents, you should offer to make photocopies for them on the Company's photocopy machine while the government agents observe. Such documents may be necessary to conduct the Company's business. Therefore, you should offer to do such copying for the government. However, whether the government allows you to do so is solely in its discretion and this does not allow you to prevent or obstruct them from taking the documents listed in the search warrant.

The government may provide you with a receipt of all documents and objects taken pursuant to a search warrant. You have a right to ask that the receipt be detailed in its description of what is taken as well as from where it was taken.

(8) You are not authorized to sign any documents on behalf of the Company. If any agent asks you to sign any document you may inform him that you cannot do so until you have had the opportunity to consult with the Compliance Manager or The Company's legal counsel.