UNBRIDLED CHANCES PSYCHOTHERAPY PROFESSIONAL CORPORATION

Policies & Procedures

INTRODUCTION

Unbridled Chances Psychotherapy Professional Corporation, (the "Company") is a California for profit professional corporation that provides psychotherapy and equine psychotherapy services to patients in the State of California. The objectives of implementing policies and procedures include the prevention and detection of improper conduct and encouraging adherence to laws. Using ethical business practices demonstrates a commitment to honesty and promotes trustworthiness. A practice's reputation is vital to staying in business. That reputation can be damaged by employees' actions. Building a compliance program will allow organizations to set standards and educate employees, thereby reducing risk and protecting their reputation.

Compliance is the responsibility of the entire Company family. Employees, contracted staff, and medical staff ("personnel") are responsible for abiding by policies, procedures and other rules and regulations.

Bringing forward concerns is imperative. No employee will face retribution solely for reporting a suspected area of non-compliance. However, failure to report may result in disciplinary action.

SUMMARY OF IMPORTANT LAWS

Health Care Fraud

Submitting false or fraudulent billing claims to private insurance or to public benefit programs such as Medicare and Medicaid can result in criminal health care fraud charges. There are federal and state health care fraud laws. Usually, these laws involve purposefully or knowingly submitting fraudulent claims. An honest billing mistake is different.

False Claims Act

The False Claims Act (FCA) prohibits submitting false or fraudulent claims to the federal government, such as billing claims to Medicare, Medicaid, and Tri-Care. Liability can arise when we are reckless in submitting a false claim, or when we should have known better.

A violation of this law can involve things like:

- Submitting a false or fraudulent billing claim
- Falsifying information to obtain a pre-authorization
- Falsifying medical records
- Keeping overpayments

The Anti-Kickback Statute

The federal Anti-Kickback Statute is a criminal law that prohibits giving something of value to induce or reward referrals. There are similar state laws prohibiting kickbacks and patient brokering.

A violation of these laws can involve things like:

- Working with certain kinds of "marketing" people
- Rewards for going to or switching to another medical provider or pharmacy (gift cards, cash, etc.)
- Giving discounts
- Waiving co-pays
- Any other freebies, discounts or financial incentives

Physician Self-Referral or "Stark Law"

The law specifically prohibits physicians from referring designated health service (DHS) to an entity that he or she, or an immediate family member, has a financial relationship with, including compensation, investment, or ownership. DHS are the following items:

1. Clinical laboratory services.
2. Physical therapy services.
3. Occupational therapy services.
4. Radiology services, including magnetic resonance imaging, computerized axial tomography scans, and ultrasound services.
5. Radiation therapy services and supplies.

6. Durable medical equipment and supplies.
7. Parenteral and enteral nutrients, equipment, and supplies.
8. Prosthetics, orthotics, and prosthetic devices and supplies.
9. Home health services.
10. Outpatient prescription drugs.
11. Inpatient and outpatient hospital services.
12. Outpatient speech-language pathology services.

This Federal law is specific to physicians and for services that are payable under Medicare or Medicaid. Referrals do not need to only be physician orders, but a physician certifying a plan of care can also qualify as a referral under the Stark Law.

Family members are also included in the law. This inclusion prevents individuals or entities from circumventing the law by referring the services to the physician's family member as opposed to directly to the physician. Medicare has a very broad definition of a family member; husband, wife, birth or adoptive child, parent or sibling; stepparent, stepchild, stepbrother, stepsister; in-laws (father, mother, son, daughter, brother, or sister); grandparent or grandchild and the spouse of a grandparent or grandchild.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The federal government established regulations for how protected health information ("PHI") would be handled and afforded specific rights to patients as it relates to their PHI.

PRIVACY AND SECURITY OF PHI

HIPAA Privacy Rule

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes standards for the protection of health information. The standards speak to how an individual's health information is used and how it is disclosed. A goal of the Privacy Rule is to strike a balance between allowing the information flow to promote quality health care while at the same time protecting peoples' privacy.

All individually identifiable health information held or transmitted by this clinic or its business associate, in any form or media, whether electronic, paper, or oral is covered by the Privacy Rule. Using or disclosing information that has been de-identified (i.e. redacted) is permitted. De-identification means the removal of all specific identifiers related to the individual or the individual's relatives, household members and employers.

According to the Privacy Rule, there are instances in which information can be disclosed without an individual's authorization. For example: providing the patient their own records; for treatment, payment, or health care operations; when it is required by law such as a court order; or as part of a government or insurance audit or investigation.

HIPAA Security Rule

The Standards for Security of Individually Identifiable Health Information (Security Rule) applies to PHI that is held or transferred in electronic form. It does not apply to information that is

transmitted orally or in writing.

The Security Rule requires that covered entities maintain appropriate administrative, technical, and physical safeguards to protect electronic forms of protected health information.

The Security Rule requires an organization to implement the following safeguards:

(1) Administrative Safeguards.

a. Risk Analysis and Management. Risk analysis and management allows an entity to determine what security measures are reasonable and appropriate. Risk analysis includes considerations of (i) the likelihood and impact of potential risks to e-PHI; (ii) documenting what security measures were taken and why; (iii) implementation of security measures to address the risks identified; and (iv) maintaining continuous, reasonable, and appropriate security measures.
b. Security Management Process. A process designed to identify areas of potential threats and vulnerabilities and implementing reasonable and appropriate measures to reduce threats and vulnerabilities.
c. Security Personnel. A security/compliance office should be appointed to develop and implement security policies and procedures.
d. Information Access Management. Access to PHI should be limited to the minimum amount necessary based on the employee's role.
e. Workforce Training and Management. Training and education of all security policies and procedures must be given and appropriate disciplinary action taken when they are violated.
f. Evaluation. A periodic review of how well the security policies and procedures work.
g. Facility Access and Control. Access to areas where PHI is stored or e-PHI can be accessed must be restricted to the minimum amount necessary based on an employee's role.
h. Workstation and Device Security. Policies and procedures must cover the proper use of and access to workstations and electronic media, and the transfer, removal, disposal, and reuse of electronic media containing or with access to e-PHI.

(2) Technical Safeguards.

a. Access Control. Individuals should only be authorized to access PHI to the minimum amount necessary based off his/her role.
b. Audit controls. Entities must have mechanisms that allow it to record and examine access and other activity in information systems.
c. Integrity Controls. PHI must not be improperly altered or destroyed and there must be a mechanism to confirm the integrity of the PHI.
d. Transmission Security. There must be a mechanism to secure e-PHI that is being transmitted over an electronic network.

More information can be accessed at:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Health Information Technology for Economic and Clinical Health Act (HITECH)

The Health Information Technology for Economic and Clinical Health Act (HITECH) was signed into law on February 7, 2009. The Act directed Health and Human Services to establish programs to improve the quality, safety, and efficiency of health care by creating a standardized process for the exchanges of health information. The Act describes notification requirements for PHI breaches, strengthened some of the privacy rights, and increased the potential penalties for covered entities and business associates who violate the HIPAA Breech Notification Rule

Breach Notification Rule

HITECH requires covered entities and their business associates to provide notification for breaches of unsecured PHI. One such provision provided clarification of when breaches of unsecured health information needed to be reported to Health and Human Services.

First, when PHI is compromised through an impermissible use or disclosure, it is presumed to be a breach unless it is demonstrated that there is a low probability that the protected health information has been compromised based on a risk assessment. Such a risk assessment should include an evaluation of:

(1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
(2) the unauthorized person who used the protected health information or to whom the disclosure was made;
(3) whether the protected health information was actually acquired or viewed; and
(4) the extent to which the risk to the protected health information has been mitigated.

A breach does not include:

(1) a person who has authorization to access information inadvertently accesses the wrong information;
(2) a person who is authorized to access information discloses the wrong information to another person who was authorized to access information; and
(3) it is determined that the individual who received the information is unable to retain the information.

For disclosures that have been determined to be a breach, notification must be made to those individuals whose information was breached, HHS, and potentially to the media. Once a breach has been discovered, individual notice must be provided and with sixty (60) days following the discovery of the breach.

HHS must be notified of all breaches. For those breaches affecting this clinic, notice may be provided on an annual basis, as this clinic's records will involve less than five-hundred (500) people.

MEDICAL RECORDS

All of the Company's medical records must be accurate and capable of providing information that documents the treatment provided and supports the claims submitted on behalf of the patient. Tampering with or falsifying medical records, financial documents, or other business records will not be tolerated.

Remember, governmental agencies often take the viewpoint that if it was not documented, it did not occur. Insufficient documentation errors occur where there is insufficient medical documentation to support the treatment or payment for the services provided. Insufficient documentation errors may include:

(1) Incomplete progress notes
(2) Unauthenticated medical records
(3) Lack of documentation of intent to order services or procedures, including medications
(4) Lack of documentation that a patient was counseled regarding a treatment decision or non-compliant patient conduct

Medicare, Medicaid and other insurance companies' provider agreements require that providers maintain records for a minimum of six (6) years.

PATIENT RIGHTS

Pursuant to the ACA, the HHS, in collaboration with other stakeholders, developed the Patient's Bill of Rights to increase patient access to care, make coverage more affordable, and help people with extra vulnerabilities to obtain care. The Patient Bill of Rights includes:

(1) The right to information about quality care and treatment consistent with available resources and generally accepted standards and the right to refuse treatment and to be informed of the consequences of his/her refusal;
(2) The right to choose a health care provider and to know, at all times, the identity, professional status, and credentials of the provider providing care;
(3) The right to emergency treatment;
(4) The right to make decision about the receipt of health care;
(5) The right to be treated with respect and to be free from discrimination for any reason, to include sex, gender, age, race, national origin, religion, sexual orientation, or disability;
(6) The right to confidentiality and to access medical records; and
(7) The right to complain about treatment, billing issues, wait times, and lack of services.

CODE OF CONDUCT

Scope: All Company employees, medical staff, and contractors (personnel) shall adhere to high standards of ethical conduct, and will comply with and assist the Company in complying with all applicable laws and regulations and third-party payor program requirements.

Ethics and accountability are core values of the Company. Patients and their family members, governmental agencies, and business partners put trust in us to do the right thing. All personnel are expected to read this Code of Conduct and the associated policies and procedures, and to acknowledge that they fully understand its requirements. This Code of Conduct does not cover all possible scenarios, nor does it provide all of the answers, but is meant to serve as a valuable resource to assist all personnel in understanding where to go if they suspect any inappropriate or unethical conduct or decisions are occurring.

Policy: **The Company** personnel shall comply with the following Code Of Conduct:

(1) Ethical and professional standards. The Company personnel shall comply with and perform their services consistent with high ethical and professional standards. They shall treat patients, co-workers, and others in a professional manner with honesty, fairness, dignity and respect.

(2) Policies and procedures. The Company personnel shall comply with all applicable policies and procedures.

(3) Laws, regulations, and program requirements. The Company personnel shall comply with all applicable federal and state laws, regulations, and third-party payor program requirements.

(4) Non-discrimination. The Company personnel shall not discriminate against other Company personnel, patients, or others on the basis of race, color, sex, religion, age, national origin, ancestry, disability, or sexual orientation.

(5) Offering or receiving items of value to induce referrals. Federal and state laws prohibit paying, offering or receiving anything of value to induce referrals for healthcare business unless certain conditions are met. The Company personnel shall not offer, solicit, pay or accept anything of value in exchange for health care referrals. This applies to offering or receiving any money, gifts, free or discounted items or services, professional courtesies, or other arrangements with the intent to induce referrals. This applies to any such transactions involving potential referral sources, including transactions with other health care providers, vendors, or patients.

(6) Financial relationships with physicians and other referral sources.

a. The Company personnel shall not enter any contract or other financial arrangement with, or give or receive anything of value to or from, an outside physician, a physician's family member, or other referral source.

b. If the Company has a contract or other financial relationship with an outside

physician or a member of the physician's family, the Company personnel shall not bill for any items or services referred by that physician without legal consultation.

c. The Company personnel must strictly comply with the terms of any approved contract or other financial arrangement with outside physicians, their family members, or referral sources. Failure to perform or improper modifications of such contracts or arrangements may violate applicable laws.

(7) Improper inducements to Medicare or Medicaid beneficiaries. Inducements to Medicare, Medicaid, or other government beneficiaries may violate applicable law. The Company personnel shall not waive or discount co-pays unless such discount complies with the Company policy. The Company personnel shall not offer any other discount, gift, free items or service, or other inducements to patients.

(8) Professional courtesies. The Company personnel shall not offer or receive any free or discounted items or services to or from other health care providers, their family members, or their office staff unless such offer is consistent with the Company's Professional Courtesy Policy.

(9) Improper billing activities. The Company personnel shall not engage in false, fraudulent, improper, or questionable billing. Such improper activities include, but are not limited to:

a. Billing for items or services that were not actually rendered;

b. Billing for or rendering items or services that were not medically necessary;

c. Submitting a claim for physician services when the services were actually rendered by a non-physician, or where a physician failed to provide the level of supervision required by applicable laws or regulations;

d. Submitting a claim with the wrong rendering provider listed thereon;

e. Submitting a claim for payment without adequate documentation to support the claim;

f. Signing a form for a physician without the physician's authorization;

g. Improperly altering medical records;

h. Prescribing medications and procedures without proper authorization;

i. Using a billing code that provides a higher payment rate than the correct billing code (i.e., "upcoding")

j. Submitting bills in fragmented fashion to maximize reimbursement even though third-party payors require the procedures to be billed together (i.e., "unbundling");

k. Submitting more than one claim for the same service (i.e., "duplicate billing").

If Company personnel have a question about the proper standard or procedure for documenting or submitting a claim, they should contact their supervisor.

(10) Unfair competition and deceptive trade practices. Federal and state antitrust laws prevent certain anti-competitive conduct, including collusive agreements among competitors to set prices; divide patient care or services; boycott other entities; etc. The Company personnel should not engage in collusive discussions with competitors over such things as

prices, employee wages, services to be rendered or eliminated, or division of patients or patient services. Similarly, the Company personnel should not discuss exclusive arrangements with third-party payors, vendors, and providers. Finally, the Company personnel should not engage in any deceptive acts or practices relating to violations of the Federal Anti-Kickback Statue, Stark, and/or any State or Federal laws and regulations.

(11) Privacy and confidentiality of PHI. The Company personnel shall maintain the confidentiality of patients' PHI as required by the Company's privacy policies and applicable law, including but not limited to HIPAA/HITECH and its accompanying regulations. The Company personnel should not access patient information unless they have a need to access the information because of their job duties.

(12) Privacy and confidentiality of Employer information. To the extent allowed by law, the Company personnel shall maintain the confidentiality of communications and records containing confidential information concerning co-workers; communications and records relating to the Company's financial or business operations, trade secrets, credentialing or peer review actions; documents prepared in anticipation of litigation; and communications with legal counsel for the Company. This section shall not be construed to prohibit activity protected by the National Labor Relations Act.

(13) Entities that contract with the Company. The Company personnel shall ensure that vendors and other entities which contract with the Company comply with the Compliance Program and cooperate with the Company's compliance efforts. Nothing in this policy shall be construed as an undertaking by the Company to inspect, assume liability for or guarantee the performance of work or activities by independent contractors or other agents.

(14) Questions concerning policies and procedures. The Company personnel shall seek clarification from or approval by their respective supervisors before engaging in actions or transactions if there is any question concerning whether the action or transaction complies with applicable laws, regulations, program requirements, or the Company's policies.

(15) Report suspected violations. The Company may have an obligation to promptly repay money it improperly receives from third-party payors within 60 days. it is essential that the Company personnel:

a. Comply with applicable laws, regulations, and policies; and

b. Immediately report suspected violations or compliance concerns to their supervisor, as set forth in the COMPLIANCE PROGRAM: Communication About Compliance Issues Policy. Anonymous reports may be to any owner. The failure to report a suspected violation may subject the Company personnel to appropriate discipline.

(16) Non-retaliation. The Company personnel shall not retaliate against any person for reporting a suspected violation of any law, regulation, program requirement or the Company policy relevant to the Compliance Program.

POLICY: REPORTING COMPLIANCE ISSUES

Policy: The Company shall maintain an open line of communication between the Company personnel and the management to ensure successful implementation of the Compliance Program and reduce any potential for fraud, abuse, and waste. No person shall be subject to retribution or disciplinary action, who in good faith reports a concern under this program, even if the investigation into the report does not find an issue.

Procedure: The Company personnel shall comply with the following procedures when reporting suspected compliance issues:

(1) *Questions*. The Company personnel may seek clarification from their supervisor if they have questions with regard to an applicable law, regulation, third-party payor program requirement, or the Company policy or procedure. Significant questions and responses should be documented and dated.

(2) *Reporting suspected violations*. The Company personnel are required to report suspected violations of the Compliance Program or any law, regulation, or third-party payor program requirement relevant to the Compliance Program. The reports must be made as soon as reasonably possible to ensure that the Company complies with appropriate deadlines for responding to suspected compliance concerns.

(3) *Preserving confidentiality*. Where known, the Company will strive to keep the identity of the Company personnel who make a report confidential; however, the Company cannot guarantee that the information will remain confidential, e.g., if government entities become involved.

(4) *Non-retaliation*. Regardless of whether a report is made anonymously or not, no person will be subject to any retribution or disciplinary action by the Company for good faith reporting under this program, even if allegations made in good faith are found to be groundless. Persons who engage in retaliatory conduct in violation of this policy shall be subject to discipline. "Good faith" means acting with an honest belief or purpose.

(5) *Documentation*. The management or their designee will log, investigate, and file every complaint or report received. Records of complaints and investigations will be maintained for seven (7) years after the investigation is closed.

(6) *Reports*. The management shall report significant or verified complaints of suspected violations to the clinic owners/Governing Board as appropriate. All persons receiving such reports shall maintain their confidentiality to the extent consistent with applicable laws, regulations, and the Company policies.

(7) *Fraud alerts*. If the management receives a Fraud Alert, Advisory Bulletin, or other publication from CMS, the OIG, or other government entity or payor that may implicate the Company, management will take immediate steps to correct the situation; and immediately inform the owner(s), who may contact legal counsel and, if appropriate, the appropriate government authority.

POLICY: AUDITING AND MONITORING

Policy: The Company will implement a self-assessment program to monitor and evaluate the compliance program. Evidence of ongoing monitoring will be maintained by the clinic manager and periodic reports will be given to the Owner and Managers.

Procedure: The following procedure will be followed while conducting auditing and monitoring:

(1) Scope. Ongoing compliance efforts may include, but is not limited to the following:

a. Periodic review of practices or actions relevant to compliance issues, including but not limited to:

i. Claims for payment;

ii. Claim denials;

iii. Contracts with potential referral sources;

iv. Advertising or marketing initiatives;

v. Gifts or inducements to program beneficiaries;

vi. Necessity, quality, and propriety of care rendered; and

vii. Receipt of and response to compliance questions, concerns, or complaints.

b. Review of government survey or inspection results.

c. Review of government guidance or directions.

d. Interviews of employees concerning possible or potential compliance issues, including exit interviews of employees who leave the Company.

e. Discussion of compliance issues in regularly scheduled meetings.

f. Confirmation that employees have been properly trained concerning compliance issues relevant to their job duties.

g. Review of significant deviations in processes or payments.

h. Formal auditing by an internal or external professional of compliance-related issues.

(2) Violations of law. In cases where monitoring, reviews, or audits reveal evidence of an actual violation of civil or criminal law or the rules and regulations of government health care programs (e.g., Medicare or Medicaid), managers will immediately notify the owners, who may consult with legal counsel and, as appropriate, notify the relevant government authority.

POLICY: INVESTIGATION AND RESPONSE

Policy: The Company will conduct investigations concerning alleged compliance problems and maintain documentation of relevant findings.

Procedure: The Company will follow the following procedure when investigating and responding to a reported issue.

(1) Record. Upon receiving notice of a potential compliance problem, the manager shall create a record as referenced in the Compliance Officer Responsibilities Policy. The record shall contain the following information:

a. the date received;

b. the manner in which the report was received (e.g., verbal, email);

c. a copy of the report, if written;

d. a brief statement of the facts alleged;

e. notes detailing and documenting a timely investigation and response; and

f. action taken and the date the action was taken.

(2) Violations of law. If the investigation discloses what appear to be violations of applicable civil or criminal laws, the managers shall immediately report the facts to the owners. Legal counsel may be contacted to determine whether disclosure or repayment to the appropriate government should be made.

POLICY: NON-RETALIATION/NON-RETRIBUTION

Policy: The Company has an open-door policy and is committed to maintaining a culture of reporting suspected areas of non-compliance.

Procedure: All Company personnel will adhere to the following:

(1) All personnel have a duty to report actual or suspected areas of non-compliance with any law, regulations, third-party payor requirement, policy, or procedure without fear of reprisals.

(2) All supervisor/managers shall maintain an open-door policy to encourage personnel to report issues.

(3) Any personnel who in good faith reports a concern to his/her supervisor/management will not be subject to any adverse disciplinary action.

(4) Any personnel, whether a supervisor or manager, must take all reports seriously and actively investigate and, to the extent possible, maintain the trust and confidentiality of the reporter.

(5) No Company personnel shall engage in retaliation, retribution, or any other form of harassment against a reporting person. Any employee found to be doing so will be subject to disciplinary action, up to and including termination.

(6) No Company personnel, including supervisors, and managers, are exempt from the consequences of wrongdoing, including violations of this policy. However, self-disclosure will be taken into consideration when determining what disciplinary action is appropriate.

POLICY: EDUCATION AND TRAINING

Policy: The Company will provide relevant training to personnel concerning compliance issues, including but not limited to applicable laws, regulations, third-party payor requirements, and the Company policies.

Procedure: All Company personnel will adhere to the following Education and Training Procedures:

(1) New Personnel. All new Company personnel, as part of an initial orientation, will receive training appropriate to the person's position and responsibilities. The training will include:

a. A copy of the Employee Handbook and Policies & Procedures, including the Code of Conduct Policy.

b. An opportunity to ask questions and receive answers.

c. The person will sign a form verifying that they have received training concerning the policies and procedures

(2) Periodic Training. The Company personnel will receive periodic or updated training concerning the Compliance Program appropriate to the person's position and responsibilities. Such training shall occur as often as appropriate. Persons who have received compliance education or training will sign a form verifying that they have received training.

POLICY: CODING AND BILLING

Policy: The Company will ensure that all claims submitted for payment are accurate and correctly identify the services ordered. The Company will not:

A. Bill for services not provided;

B. Bill for services not properly ordered;

C. Misrepresent a patient's diagnosis to justify services;

D. Knowingly apply for duplicate payment or payment from duplicate payors for the same service;

E. Unbundle charges;

F. Misrepresent the services rendered, the amounts charged, the identity of the person receiving the service, or the identity of the person actually providing the service;

G. Utilize the billing number for a provider who did not actually provide the service;

H. Bill as if services rendered one day were rendered on different days; or

I. Take other action that is false or in violation of applicable laws or regulations.

Procedure: The Company will follow the following procedure when submitting codes and billing for services:

(1) Clinical providers and the billing department are responsible for ensuring the appropriateness of codes for any tests ordered.

(2) Questions about code selection should initially be presented to the supervisor; the ordering practitioner will be contacted if necessary.

(3) Bulletins and transmittals from third-party payors will be maintained in a designated file for ten (10) years.

(4) Ordering practitioners will ensure that the codes used are those which most accurately describe the ordered test. Codes will never be selected solely to maximize reimbursement.

(5) The Company will not:

a. Use diagnostic information provided from earlier dates of service, except in cases where approved standing orders are utilized;

b. Use prepared sheets that provide diagnostic information which has been found to be successful in maximizing reimbursement in the past;

c. Use any computer-based or other programs which automatically insert diagnosis codes without receipt of current diagnostic information from the practitioner; or

d. Assume or "make up" diagnostic information for claims submission purposes.

(6) The Company will not bill Medicare beneficiaries for non-covered tests unless a

beneficiary acknowledgment executed by the patient prior to the performance of the test is on file.

POLICY: REFERRALS

Policy: The Company helps coordinate care, treatment, and community-based services based on the patient's needs. However, many types of referrals may prohibited if the facility/provider has a financial relationship with the provider/entity or is receiving payment, in money or otherwise. The Company does not offer, pay, accept, or request any remuneration, either in cash or otherwise, for referrals for patients. This policy applies to all referrals made by Company personnel.

Purpose: The Company personnel shall follow the following procedures when making referrals:

(1) Financial Arrangements.

a. All arrangements with any outside providers or suppliers must be in writing, signed by an authorized the Company representative and the outside party, and will be reviewed by legal counsel prior to execution.

b. To the extent possible and consistent with the Company's high standard of care, patients should not be referred to entities if the Company or the provider or an immediate family-member of the provider has a financial interest in or is otherwise compensated by that provider/entity.

c. Patients will be informed that they always have a choice of provider when being referred for tests or other services or supplies.

(2) Gifts to/from Referral Sources. Any non-monetary gifts provided to or received from a referral source cannot exceed $300 in a year, cannot vary or take into account volume or value of referrals or other business, cannot be solicited by the referral source or the Company or the Company personnel, and cannot be provided to induce referrals to or from the Company. In gifts to or from a referral source must be approved by the management.

(3) Patient Gifts. Patient gifts are generally prohibited. There may be exceptions such as Christmas or other holiday gifts of nominal value. Any gifts provided to patients must be approved by the owners.

POLICY: MEDICAL RECORDS

Policy: The Company recognizes that medical records are also legal documents. Information in medical records is used to review, study, and evaluate the care a patient has received. All medical records will be neat, accurate, and readily accessible for the purpose of providing treatment and services, audits, and possible litigation proceedings.

Procedure: All Company personnel shall follow the following procedures when using medical records:

(1) Documenting Services.

a. A medical record shall be maintained for every individual who is evaluated or treated as a patient at the Company.

b. All entries will be legible and, if hand written, done in blue or black ink.

c. All entries will be dated and signed, whether electronically or by hand.

(2) Confidentiality. The medical record is a confidential document and protected from unauthorized disclosures.

(3) Content.

a. Medical records shall contain all state and federal legal, regulatory, and accreditation requirements, including but not limited to the Medicare Conditions of Participation, 42 CFR Part 482.

b. All documentation and entries in the medical record, whether paper or electronic, must be identified with the patient's full name and a unique identifier.

c. All Medical Record entries should be made as soon as possible after the care is provided, or an event or observation is made, at a minimum with twenty-four (24) hours. An entry should never be made in the Medical Record in advance of the service provided to the patient. Pre-dating or backdating an entry is strictly prohibited.

(4) Authorized Personnel. Only the following personnel may make a clinical note for a medical record:

a. Physician;

b. Nurse, including advance practice registered nurse;

c. Physician's assistant; and

d. Medical assistants.

(5) Ownership, Responsibility, and Security of Medical Records. All medical records of the Company patients, regardless of whether they were created at or received by the Company; as well as patient lists and financial information, are the property of the Company.

a. The patient and/or his or her legal representative have a right to access the information contained within the record.

b. All personnel are responsible for assuring there is a completed and accurate medical record for every patient.

c. Original copies of medical records may not be removed from the Company except by court order, subpoena, or as otherwise required by law, as further discussed in the Response to Governmental Requests Policy.

d. Medical records shall be maintained in a safe and secure area. Computers or other endpoints with access to electronic health records (EHR) shall be logged/turned off when personnel are no longer using the computer.

(6) Maintenance, Retention, and Destruction of Medical Records. All medical records will be maintained for a period of seven (7) years from the date of the last service. Prior to the destruction of medical records, reasonable attempts will be made to contact the patient prior to any destruction of any medical records.

(7) Corrections and Amendments of Records. When an error is made on a medical record, information will not be adjusted or changed except under limited circumstances.

a. Hard Copy Records.

i. Labels or liquid paper/correction fluid (such as Wite-Out) shall not be placed over entries for correction of information.

ii. If information in a paper record must be corrected or revised, draw a line through the incorrect entry so that the original information is still visible, and annotate the record with the date, the reason for the revision, and signature or initials of the person making the revision.

b. Electronic Records.

i. Adding an addendum to the electronic document must indicate the corrected information, the identity of the individual who created the addendum, the date created, and the electronic signature of the individual making the addendum.

ii. Preliminary/draft versions of transcribed documents may be edited by the author prior to signing.

iii. Once a transcribed document is final, it can only be corrected in the form of an addendum affixed to the final copy as indicated above. Examples of documentation errors that are corrected by addendum include: wrong date, location, duplicate documents, incomplete documents, or other errors. The amended version must be reviewed and signed by the provider.

iv. Sometimes it may be necessary to re-create a document (e.g., wrong work type) or to move a document; for example, if it was originally posted incorrectly or indexed to the incorrect patient record.

c. Late Records.

i. Identify the new entry as a "late entry."

ii. Enter the current date and time. Do not attempt to give the appearance that the entry was made on a previous date or an earlier time. The entry must be

signed.

iii. Identify or refer to the date and circumstance for which the late entry or addendum is written.

iv. When making a late entry, document as soon as possible. There is no time limit for writing a late entry; however, the longer the time lapse, the less reliable the entry becomes.

d. "Copy-and-Paste" Guidelines:

i. The copy-and-paste functionality available for records maintained electronically eliminates duplication of effort and saves time, but must be used carefully to ensure accurate documentation and must be kept to a minimum.

ii. Copying from another clinician's entry: If a clinician copies all or part of an entry made by another clinician, the clinician making the entry is responsible for assuring the accuracy of the copied information.

iii. Copying test results/data: If a clinician copies and pastes test results into an encounter note, the clinical-provider is responsible for ensuring the copied data is relevant and accurate.

iv. Copying for re-use of data: A clinician may copy and paste entries made in a patient's record during a previous encounter into a current record as long as care is taken to ensure that the information actually applies to the current visit, that applicable changes are made to variable data, and that any new information is recorded.

v. Information pertinent to that individual visit — including but not limited to the chief compliant, documentation of aggravating factors, relieving factors, duration, character, timing, onset of pain, and vital statistics — should never be copied and pasted.

POLICY: CONFIDENTIALITY AND PRIVACY

Policy: The Company recognizes the sensitivity of patient medical records and understands that under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), it has a duty to ensure the confidentiality and security of patient health and financial from any unauthorized, whether intentional or unintentional, use or disclosure.

Procedure: The Company shall follow the following protocol when handling protected health information:

(1) PHI may not be disclosed or released without a complete and valid written authorization signed by the patient, the patient's parent, or legally authorized representative, unless (i) the use of the PHI is for treatment, payment, or healthcare operations, or (ii) release is specifically authorized by law.

(2) Individually Identifiable Information. The following list of individually identifiable information may constitute PHI when linked with health or medical information:

a. Names of the individual, family members, employers, or household members;

b. Geographic information, such as addresses, city, county, states, or ZIP codes;

c. Dates, including birthdates, treatment dates, date of death;

d. Telephone, mobile, or fax numbers;

e. Email addresses;

f. Social Security numbers;

g. Medical record numbers;

h. Health plan beneficiary numbers;

i. Account numbers

j. Certificate/license numbers;

k. Vehicle identifiers;

l. Device identifiers

m. URLs;

n. IP addresses;

o. Biometric identifiers;

p. Full-face photographs;

q. Any other unique identifying information.

(3) Protected Health Information. PHI is any individual identifiable health or financial information, whether verbal, written, electronic, or otherwise recorded or documented, in any form or medium, that:

a. Is created or received by a health care provider, health plan, employer, or healthcare clearinghouse; and

b. Relates to the past, present, or future physical or mental or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of health care to an individual; and

i. that identifies the individual; or

ii. with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(4) The Company and its personnel are expected to treat all PHI as confidential. When disclosing information:

a. Ensure that the disclosure is either authorized by the patient, the patient's parent, or a legally authorized representative or is released in a manner required or permitted by law;

b. Release only the reasonable minimum amount of information required;

c. Take appropriate steps to prevent the unauthorized re-disclosure of PHI.

(5) Confidentiality Statement. All Company personnel are required to sign a confidentiality statement before being granted access to PHI. Personnel shall only access the minimum necessary amount of PHI required to perform the functions of his/her position.

(6) Business Associates. When working with outside contractors, the Company personnel will utilize an appropriate business associate agreement.

POLICY: INTERACTIONS WITH GOVERNMENT AGENCIES AND OFFICIALS

Policy: The Company has a policy that any contacts with governmental agencies or officials shall be conducted in an honest manner and that the Company and its personnel shall cooperate fully with all federal, state, and local governmental agencies, officials, or representatives.

It is important to remember, however, that many laws, such as 42 CFR Part 2 confidentiality provisions for substance abuse treatment records, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"), and the Physician-Patient Privilege may have conditions which must be met before information is released pursuant to some governmental request.

All such interactions shall be conducted in full compliance with all applicable laws and regulations. Any attempt to influence the decision-making process of governmental agencies or officials by an improper offer of any benefit is absolutely prohibited. This policy extends to all Company personnel. This policy covers what to do in the following scenarios:

(1) Telephone calls or receipt of letters from governmental agencies, officials, and representatives;

(2) Requests for interviews of Company personnel;

(3) Request for documents;

(4) On-site visits or inspections of the Company's practice by a governmental official;

(5) Presentation of demand letters, subpoenas, or search warrants; and

(6) Visits to the homes or other locations of employees by governmental officials.

Procedure:

(1) If the Company or any personnel are contacted by a governmental agency or official, that person should (1) immediately contact the manager who shall contact the owners; and (2) ask to see the credentials or other proper identification before speaking with the agency.

(2) Request for Interviews.

a. Interviews of Company personnel may be requested by a governmental agency or official. The managers and owners shall immediately be notified of such a request and may be consulted regarding any such request.

b. If an employee decides to be interviewed, the employee should always be truthful, cooperative, and polite and can choose to have counsel of his/her choosing present.

c. If the employee does not know with certainty the answer to any question, it is appropriate for the employee to state that he or she does not know the answer to the question. In addition, the employee may choose to stop the interview at any time.

d. No Company employee will face retaliation from the Company or any affiliated personnel based off a decision to grant or deny an interview.

(3) Requests for Documents.

a. Responding to All Documentary Requests. If a governmental agency or official presents or sends the Company or an employee a written request seeking documents, an employee should:

1. Ask the governmental official to present proper identification (if they arrive in person);
2. Obtain a business card OR write down: the name and title of the official, the government agency they represent, and contact information;
3. Write down the date and time of receipt of the request;
4. Immediately notify management of the request;
5. Do not respond to the request without first discussing it with, and obtaining authorization from, a manager; and
6. Managers should immediately notify the owners of all requests before taking further action.

b. Responding to a Search Warrant. If a search warrant is presented, the official has the authority to enter the premises, to search for evidence, or to seize documents or other items listed in the warrant. If law enforcement enters the premises with a search warrant, the employee must:

1. Ask for a copy of the search warrant and, if available, the affidavit providing the reasons the warrant was issued;
2. Ask to see the identification of the law enforcement official;
3. Politely request an opportunity to consult with a manager, owner, or corporate counsel;
4. Immediately notify a manager, owner, or corporate counsel;
5. NOT interfere in the execution of the warrant;
6. If possible, document what was searched, what was taken, whether the officials interviewed any employees or patients;
7. Not sign anything on behalf of the Company unless specifically authorized by the owners; and
8. Obtain a copy of the "inventory" of the property seized, which must be provided by the law enforcement agents.

(4) Preservation of Data. Upon notification that a governmental agency or official has requested documentation:

a. The managers and owners shall make a good faith attempt to identify potentially relevant documentation, regardless of whether it is privileged or confidential.

b. The managers and owners shall issue a notice to all relevant employees that

reasonable efforts must be made to ensure that requested documentation/data is not to be destroyed or altered in any way ("Preservation Notice").

c. Any Preservation Notice will apply equally to hard copy documentation, electronic or digital data, or documentation or data maintained at an offsite facility.

CONFIDENTIALITY AGREEMENT

I hereby acknowledge and agree that any information or documentation:

1. That has been or will be furnished to me;
2. That I have created or will create; and
3. That I have obtained or will obtain

During my employment with the Company, is confidential and sensitive. I will maintain the confidentiality of such information or documentation and will not discuss it with nor furnish it to anyone other than as authorized by the managers or owners.

Employee name (print): _____

Employee signature: _____

Date: _____

THIS FORM MUST BE COMPLETED, SIGNED AND
RETURNED TO YOUR SUPERVISOR

ACKNOWLEDGEMENT OF RECEIPT OF POLICIES & PROCEDURES

I have read and understand that:

- This policy manual replaces all previously issued editions;
- It is my responsibility to become familiar with the contents of this policy and procedure manual;
- I can ask questions and seek clarifications about the content through my supervisor; and
- The Company retains the right to modify, suspend, interpret or cancel any of the contents of this manual.

Further, I acknowledge that I have received a copy of the Company's Policy & Procedure Manual & Code of Conduct in either hard copy or electronic copy form and understand that this manual is not an employment contract and in no way guarantees my employment.

Employee name (print): _____

Employee signature: _____

Date: _____

THIS FORM MUST BE COMPLETED, SIGNED AND
RETURNED TO YOUR SUPERVISOR