Comprehensive Systems, Inc.

Corporate Compliance Program

Board Approved
4/27/2006

Reviewed 08/27/10, 05/20/11, 12/14/12, 11/15/13, 04/16/14, 01/22/15, 02/11/16, 02/23/17, 04/21/17, 04/12/19, 11/05/20, 10/22/21, 03/23/22, 03/06/24
Revised 11/07/11, 01/20/12, 10/20/14, 01/20/15, 04/07/15, 05/01/15, 01/12/18, 11/15/19, 02/21/20, 01/22/21, 04/05/23

P0307

Comprehensive Systems, Inc.
Corporate Compliance Program

Table of Contents

Corporate Compliance Policy

Comprehensive Systems, Inc. (CSI) is dedicated to the delivery of services in an environment characterized by strict conformance with the highest standards of accountability for administrative, business and financial management, HIPAA privacy and quality of care.

The leadership of Comprehensive Systems, Inc. is aware of and fully committed to the organization clearly establishing expectations regarding employee behavior, i.e., to act in a way that always respects laws and regulations and in a manner that will protect the organization's assets from fraud, waste, and abuse. The development and implementation of policies and procedures and other corporate compliance measures will help ensure regular monitoring and conformance with all legal and regulatory requirements.

On April 27, 2006, the Board of Directors of Comprehensive Systems, Inc. passed a resolution directing and authorizing the Executive Director to take all actions necessary to immediately and fully develop and implement a Corporate Compliance Program for the company.

Effective also on this date, the Board passed an additional resolution designating and appointing the Corporate Compliance Director (CCD) for Comprehensive Systems, Inc. The CCD will have direct access to the Executive Director, legal counsel and the Board of Directors as necessary. In addition to development, implementation, and monitoring of the Corporate Compliance Program, the CCD shall be responsible for establishing and chairing the Compliance Committee meetings and submitting periodic reports on the committee's activities and other corporate compliance activities as required.

Role of the Corporate Compliance Director

The Board of Directors has designated a Corporate Compliance Director for Comprehensive Systems, Inc. The Corporate Compliance Director has the authority and responsibility for overseeing the development, implementation and maintenance of Comprehensive Systems, Inc.'s Corporate Compliance Program. The Corporate Compliance Director reports to the Board of Directors regarding compliance related activities, results of internal auditing activities, results of investigations regarding suspected fraud, waste and abuse from personnel. Ethical and legal behavior, including adherence to all of Comprehensive Systems, Inc. policies and procedures, is not the sole responsibility of the Corporate Compliance Director. All employees play a critical role in the organization's commitment to ethical and legal compliance and to the success of the Corporate Compliance Program.

Role of the Compliance Committee

The Compliance Committee is responsible for implementing the activities of the Corporate Compliance Program under the direction of the Corporate Compliance Director. The members of the Compliance Committee will provide advice on how to achieve the goals and objectives of the Corporate Compliance Program. The committee provides direction and consults with the Risk Manager on the Risk Management Plan/Disaster Recovery Plan/ Emergency Preparedness Plan. Committee members are expected to display integrity, confidentiality and professional judgment. The Compliance Committee consists of eight core members, including the Corporate Compliance

Director, Legal Counsel, Associate Director, Executive Director, HR Director, Program Director, QA Director, IT Coordinator and Risk Manager. This committee meets on a quarterly basis as a minimum.

Corporate Compliance Program Policies and Procedures

Comprehensive Systems, Inc. has adopted policies and procedures implementing the Corporate Compliance Program which includes Detecting and Preventing Waste, Fraud and Abuse, Code of Conduct, HIPAA Privacy, and Quality of Care. All employees of Comprehensive Systems, Inc. will receive training on the policies and procedures of the Corporate Compliance Program and will be required to sign a written acknowledgment that they have received, read and will abide by the policies and procedures outlined in this program. New employees will receive compliance training during orientation. All employees receive compliance training on an annual basis.

Departmental Policies and Procedures

Neither the Corporate Compliance Program nor the Code of Conduct covers all of the detailed policies and procedures adopted by Comprehensive Systems, Inc. to achieve compliance in each area of its operations. Policies and procedures pertaining to specific areas of the organization's operations will be reviewed and, where necessary, amended or created to ensure clarity of and adherence to legal and ethical requirements governing that particular area. Employees affected by these policies will receive training on the policies and procedures specific to their job responsibilities. Departmental policies and procedures are located in each of the respective departments. Questions concerning the location of a particular policy or procedure, or concerning a policy's meaning, should be directed to the department supervisor.

Code of Conduct Policies and Procedures

Comprehensive Systems, Inc. has adopted a Code of Conduct, setting forth the legal and ethical standards of the organization, to be followed throughout the organization for the purpose of reducing unlawful or unethical conduct in the workplace. Each year, all employees, board members, and volunteers of Comprehensive Systems, Inc. will receive and review the Code of Conduct. (See P307.1) Each will be required to sign a written acknowledgment that he/she has received, read, and will abide by the organization's Code of Conduct. The signed acknowledgment will be maintained by Comprehensive Systems, Inc. in the appropriate file.

Detecting and Preventing Medicaid Waste, Fraud and Abuse

Federal and state laws prohibit waste, abuse and fraud of Medicaid funds that Comprehensive Systems, Inc., receives for services provision. These laws include the 2005 Deficit Reduction Act and False Claims Act (amended 1986). At Comprehensive Systems, Inc. Medicaid funds are received for Intermediate Care Facility for Individuals with Intellectual Disabilities (ICF/IID), Habilitation Services, and Home and Community Based Waiver Services (HCBS).

Comprehensive Systems, Inc. (CSI) strictly prohibits Medicaid waste, abuse, and fraudulent practices. The leadership of CSI is aware of and fully committed to the organization clearly establishing expectations regarding employee behavior, i.e. to act in a way that always respects laws and regulations and in a manner that will protect the organization’s assets from fraud, waste and abuse. The leadership of CSI strongly believes that the development and implementation of policies and procedures and other corporate compliance measures will help ensure regular monitoring and conformance with all legal and regulatory requirements.

Medicaid waste, abuse or fraud may include, but are not limited to:

- Billing for services that were never provided

- False cost reports whereby inappropriate expenses not related to services provision are intentionally included in cost reports
- An illegal kickback, where a provider may conspire with another provider to share part of monetary reimbursement the provider receives in exchange for service referrals. Such kickbacks could include cash, vacation trips, automobiles, or other items of value.

False Claims Act "Whistleblower Protection" – Non Retaliation

The False Claims Act contains language protecting "whistleblower employees," who report suspected Medicaid waste, abuse and fraud, from retaliation by their employer. Employees that are discharged, demoted, suspended, threatened, harassed or in any way discriminated against in the terms and conditions of employment by the employer for blowing the whistle are entitled to recover all relief necessary to make the employee whole. Damages available to the employee that proves retaliation include: reinstatement, two times back pay, interest, emotional distress damages, costs, and attorney's fees. Additionally, the successful whistleblower may be eligible to recover 15% to 30% of the government's recovery from the fraudulent practice. The False Claims Act allows a private person to file a lawsuit on behalf of the United State government against a person or business that has committed the fraud.

Any employee who feels they are being retaliated against for reporting Medicaid waste, abuse or fraud should immediately report this concern to the Corporate Compliance Director. CSI will implement appropriate protective actions for the employee. An internal investigation will be initiated immediately with suitable corrective actions taken as a result of the investigative findings. Documentation related to founded allegations will be maintained in the Corporate Compliance Director's confidential records.

Mechanisms and Procedures for Detection and Prevention

CSI has key mechanisms and procedures in place to detect and prevent Medicaid waste, abuse, fraud, and improper documentation including:

- Annual External Audit completed by an outside Certified Public Accountant for all Medicaid funded services.
- An outside CPA completes all Medicaid prospective and annual cost reports submitted to DHS.
- Samples of Medicaid service logs are reviewed each month by the Internal Auditor prior to billing for services, insuring documentation meets rules and regulations prior to billing for services. Corrective actions are implemented as needed to improve the quality of Medicaid documentation.
- Initial and Annual Training is provided to all employees on detecting and preventing Medicaid abuse, waste, and fraud including reporting procedures.
- Each month, Quality Assurance staff completes random reviews of Medicaid service logs from the CSI service areas. Reports are generated which include any corrective actions needed to improve the quality of documentation.

Documentation

CSI monitors Medicaid documentation in order to detect and prevent improper payments for Medicaid services.

Improper payments may include:

- Payment for services when the service provision is not adequately documented. A service that is not adequately documented should not be billed to Medicaid. CSI has implemented an audit process to monitor documentation.
- Medically unnecessary services due to lack of documentation in medical records to support eligibility and need for services. CSI nursing, Accounts Payable, and Admissions verify any medical procedures.

- Incorrect coding when billing for services and/or using the wrong code for a particular service. CSI has implemented an audit process to verify billing.
- Non-covered costs or services that do not meet the state of Iowa's reimbursement rules and regulations. These are services that are not medically necessary.
- Third party liability is where a private insurance company or another payer, was the primary payer and Medicaid was billed instead. CSI Accounts Payable and Unit/Home Administrators are responsible for making sure the appropriate entity is billed.

GIFTS, GRATUITIES AND CONFLICT OF INTEREST

Comprehensive Systems, Inc., its employees and agents, are prohibited from offering or receiving cash, gifts, or gratuities that are likely to influence the decisions or judgments of those receiving such payments or gifts, in conflict with the best interests of Comprehensive Systems, Inc. or the people it serves.

Individuals, Prospective Individuals and Families

Employees and volunteers of Comprehensive Systems, Inc. may not solicit or accept any gift, money, donation, or other item of value from any individual, an individual's family member or prospective individual for any item or service provided by the facility or in exchange for admission to the facility. Individuals or individuals' family members may want to offer gifts of nominal value (e.g., tips, candy, food, flowers) to individual employees of Comprehensive Systems, Inc. to express their gratitude for the care and compassion provided by the employees. Refusing these nominal gifts may be upsetting to individuals, or individuals' family members, who want to express their gratitude in this way. Employees may accept such gifts from a individual, or a individual's family member, provided that such gifts are infrequent and of nominal value, and when acceptance of such gifts does not violate professional standards of ethical conduct governing the employee's professional relationship with the individual. Any such gift must be made in the presence of the employee's immediate supervisor and must be made and received in good faith.

Employees and agents may not solicit individuals (or individuals' family members, representatives, or friends) for contributions or donations of money or gifts for the personal benefit of the employee or agent, or the employee's family or friends.

Employees may not accept a bequest from a former individual. Individuals who wish to make a bequest to individual employees will be encouraged to make the bequest to a fund established for the benefit of all employees.

Vendors, Business Partners, Service Providers

Comprehensive Systems, Inc. is committed to the concept of transparency in all dealings with vendors, business partners, service providers, etc. Employees and agents of Comprehensive Systems, Inc. may not solicit or accept any money or other consideration (including cash, gifts, commissions, bonuses, gratuities, travel, rebates, kickbacks, or bribes) from a person or business providing, or seeking to provide, goods or services to Comprehensive Systems, Inc. Any such gift should be returned immediately to the provider with a letter explaining this policy.

Employees and agents may accept non-cash gifts of nominal value, such as pens, coffee mugs, and other similar novelties, from a provider of goods or services when circumstances show that the gifts are offered as a business courtesy only and not as an inducement to do business with the provider. Acceptance of cash or cash equivalents, such as gift certificates or discounts, offered to employees or agents by providers of goods or services in any amount is strictly prohibited.

Employees and agents may not offer or pay any money or other consideration (including cash, gifts, commissions, bonuses, gratuities, rebates, kickbacks, or bribes) to any person or business for the purpose of inducing the person or business to refer individuals to Comprehensive Systems, Inc. for items or services that may be reimbursed under the Medicaid program.

Comprehensive Systems, Inc. may solicit, accept, or receive a charitable, religious, or philanthropic contribution from an organization or from a person but only to the extent that the contribution is not a condition of admission or expedited admission for a Individual or prospective Individual and provided that the contribution is made for the benefit of all Individuals.

Comprehensive Systems, Inc. may accept non-cash, perishable gifts (e.g., food, candy and flowers) from a provider of goods or services which are given for the benefit of all employees, or a group of employees, provided that such gifts are infrequent and of nominal value per recipient, and when circumstances show that the gifts are given as a business courtesy only and not as an inducement to do business with the provider.

Conflict of Interest – Employees

Employees and agents of Comprehensive Systems, Inc. who hold a five percent or greater financial interest in an entity doing business with Comprehensive Systems, Inc., or who are related to any person holding a five percent or greater financial interest in an entity doing business with Comprehensive Systems, Inc., must report this information to the employee's supervisor or to a member of the compliance committee.

Conflict of Interest – Board or Directors

Any duality of interest or possible conflict on the part of any member of Comprehensive Systems, Inc. Board of Directors shall be disclosed to the other board members and made a matter of record as soon as such conflict is determined to exist. On an annual basis (December Board meeting), each Director shall sign a Conflict of Interest statement as set forth below.

Any board member having duality of interest or possible conflict of interest on any matter shall not vote or use his/her personal influence on the matter. Such Director shall still be counted in determining the quorum for the meeting. The minutes of the meeting shall reflect that a disclosure was made as well as the abstention from voting. The forgoing shall not be construed as preventing the board member from answering questions of other board members since his/her knowledge may be of great assistance. (See P0209)

Personal Fundraising

At the discretion of the Executive Director, the Associate Director or their designee, company sponsored fundraising activities may occasionally be conducted on company property during working hours and in work areas, which may include the use of a limited amount of work time and company state resources.
In addition to the company sponsored activities, employees will be allowed to conduct other fundraising activities in non-work areas and on non-work time.
Employees will be allowed to post information such as personal items for sale, fundraising activities, and community events in non-work areas on non-work bulletin boards.
External individuals and organizations will not be allowed to conduct fundraising activities on company property.
Solicitation will not be allowed on company property, except as specifically otherwise provided for in this policy. (See P0116)

Purchasing, Selling & Borrowing

Comprehensive Systems, Inc. staff shall not purchase, use or borrow items from individuals. Additionally, staff shall not sell items to individuals. Comprehensive Systems, Inc. staff shall not ask individuals to buy items for them or intimidate individuals into buying items for them. This practice is financial exploitation, which is against the law. Failure to follow this policy will result in disciplinary action which could include termination. (See P0362)

Witnessing of Documents

Individuals, their families or representatives are encouraged to have any document which requires a witness or notarization executed by an outside individual not affiliated with Comprehensive Systems, Inc. The process of witnessing any document will be undertaken only in emergency circumstances. When a witness signature is required in an emergency situation, such document shall be signed only by a manager or officer of the company. Under no circumstances should any staff member or healthcare professional involved with the individual's care undertake the task of witnessing a signature. In the event the witnessing of the execution of a document includes an assessment of mental capacity or state, only the Executive Director or Associate Director, in their sole discretion, shall be allowed to witness. This however, shall not require them to witness any document. No staff member shall witness any advance Directive or Living Will for any individual. (See P0117)

Employee Relationships

It shall be the policy of Comprehensive Systems, Inc. that no management employee of the company shall enter into or maintain any type of romantic or dating relationship with any other employee of the company over whom the management employee has any supervisory duties or responsibilities. This policy does not prevent employees from having a purely social relationship outside the work place, but rather this policy is intended to promote a professional atmosphere and to avoid potential conflicts of interest and the appearance of impropriety on behalf of any employee.

Supervisory/managerial employees shall not supervise close relatives i.e. parents, step-patents, children, step-children, grandchildren, spouse, brothers, sisters, legally adopted children, step-brothers, step-sisters, mothers-in-law, fathers-in-law, grandparents, aunts, uncles, spouse's grandparents or grandchildren. Exceptions can be made with approval by the Board of Directors. In the HCBS areas, family members may work with related individuals.

It shall be the policy of Comprehensive Systems, Inc. that no employee of the company shall enter into or maintain any type of romantic or dating relationship with an individual. If there is a violation of this nature, discipline action will occur which may result in termination. (See P0344)

Survey Conduct

Comprehensive Systems, Inc. is periodically surveyed by representatives from the Department of Inspections and Appeals to determine that it is complying with all state laws, rules and regulations and is providing quality care to its individuals. The objectivity of the survey process and of the person conducting the survey is essential to ensure that a fair and accurate report is made by the regulating agency.

In order to preserve the integrity of the survey process and to avoid any appearance of improper influence, it is the policy of Comprehensive Systems, Inc. that its employees shall refrain from social contact with survey officials while they are engaged in a survey of any facility of Comprehensive Systems, Inc. Comprehensive Systems, Inc. will advise survey officials of this policy if necessary to make them aware of the potential consequences to an employee arising from violation of this policy. (See P0346)

Acceptable Use of Social Media
Comprehensive Systems, Inc. is committed to promoting appropriate interactions with the public and with each other when using social media. It is the expectation that all employees follow the Social Media Policy (P0371) which outlines honesty, respect, confidentiality of persons served, community and applicable compliance laws/regulations. Inappropriate actions that result in violation of the code of conduct or other agency policies may result in discipline action up to and including termination.

Advocacy Efforts for Persons Served
Efforts will be made to ensure language and cultural differences are not barriers to participation in services. Individuals will be provided access or referral to social, legal or economic advocacy resources. (See P1145)

Corporate Citizenship
The Administration of Comprehensive Systems, Inc. is committed to promoting involvement in community organizations for employees and individuals served such as Chamber of Commerce, Rotary Clubs, Meals on Wheels, etc.

Employment
CSI will not hire any individual who is on the Abuse Registry or Office of Inspector General (OIG) or System for Award Management (SAM) Exclusion Lists. If a criminal record exists, DHS will determine if the individual is eligible for employment. During the course of employment, it will be the responsibility of the employee to notify the employer within 48 hours of founded charges of child or dependent adult abuse, any criminal convictions that they are found guilty of or if they are placed on the OIG or SAM Exclusion List. The Iowa Department of Human Services (DHS) will determine if the employee can remain employed at CSI in accordance with the Iowa Code. If determination is made by Iowa DHS that the employee is prohibited from working at CSI, the employee will be terminated. If the employee is added to the OIG or SAM Exclusion List, they are not allowed to work for CSI and will be terminated.

Acceptable Use for HIPAA Privacy

This policy reflects Comprehensive Systems, Inc.'s commitment to inform employees of their responsibilities to protect the confidentiality, integrity and availability of the organization's electronic protected health information (EPHI).

Comprehensive Systems, Inc. employees are responsible for taking all reasonable precautions to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI) for which they have access. In addition, Comprehensive Systems, Inc. employees must receive appropriate security training before accessing EPHI on any company computer or network system, workstation, or other electronic device. Non-compliance with this policy can lead to the application of the organization's discipline policy.

This policy is applicable to all employees that access, use or disclose electronic protected health information for any purposes. The scope of this policy includes all protected health information in electronic form.

PROCEDURE
The following standards and safeguards must be implemented to satisfy the requirements of acceptable use:

1. *Your Role in Protecting EPHI:* You are responsible for taking all reasonable precautions to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI) for which you have access. At a minimum, these precautions require that you:

- Must not share your account or your password: All activities associated with your assigned user account are your responsibility
- Must report any suspicious activity involving your account or other systems with access to EPHI
- Must not circumvent or otherwise bypass existing security measures: For example, do not disable anti-virus or firewall software

2. *HIPAA Security Training:* You must receive training on HIPAA security issues before accessing your computer accounts or Comprehensive Systems, Inc. information systems containing EPHI. In addition, you must attend training on an annual basis or more frequently as needed. Such training will consist of, but is not limited to:

- Responsibilities of employees for protecting EPHI
- Security best practices (e.g. how to choose a good password, how to report a security incident).
- Comprehensive Systems, Inc. information security policies and standard

3. *Protecting Your Workstation:* You must protect your workstation and the EPHI for which you have access from unauthorized access. Workstations are defined in this policy as desktop computers, laptops, personal digital assistants (PDA), and other electronic devices that you may use to access EPHI. At a minimum, you:

- Must not open email attachments without verifying with the sender
- Must not download or install any software not required for official job duties
- Must ensure anti-virus software is installed and regularly updated
- Must ensure that your workstation is physically located in a manner that minimizes the risk that unauthorized individuals can gain access: In addition, be sure that your monitor or display screen is positioned to prevent viewing by unauthorized individuals
- Must log off from your workstation when your shift is complete.
- Must ensure that your workstation is locked when unattended: This may be done manually or by automated screen locking software
- Must store all media (e.g. encrypted flash drives) that contain EPHI in a secure location: When disposing of media with EPHI, the data must be removed with data sanitizing software or the media must be physically destroyed
- All flash drives must be encrypted
- When transporting laptop computers, they must be stored in the trunk of the vehicle or in a locked container out of view when unattended. Vehicle doors must also be locked.

4. *Storing EPHI on your workstation:* If possible, do not store EPHI on your workstation. Use other alternatives, such as storing the EPHI on a secure server or a secure network storage device. However, if you store EPHI on your workstation, the following requirements apply to you:

- You must obtain approval from your manager prior to storing EPHI on your workstation.
    - Your manager must inventory and document the EPHI stored on your workstation at least on an annual basis.
    - Your manager must review and document the security safeguards for protecting the EPHI stored on your workstation.
- You must encrypt the data files containing EPHI wherever possible
    - If encryption is not possible, you must obtain a review by the HIPAA Security and Privacy Officer prior to storage.
- If you are storing EPHI on a portable device, such as a PDA, you must encrypt the data to protect it from unauthorized disclosure in the event the device is lost or stolen.

5. *Email and EPHI:* Do not send EPHI over email unless you take reasonable precautions to protect the EPHI. At a minimum you must (a) if you send the email from your company email account on the company's enterprise email system to another company email account on the company's enterprise email system and implement the appropriate privacy controls or (b) if you send email from your email account to locations outside of the enterprise email system, implement the appropriate privacy controls and encrypt the mail with a recommended encryption solution. Contact the HIPAA Privacy Officer if you have questions concerning privacy requirements.

6. *Wireless Networking and EPHI:* Do not access or send EPHI over a wireless network, unless the data is encrypted prior to transmission. Data sent over an unencrypted wireless network can be captured by unauthorized persons in nearby buildings, parking lots, and streets.

7. Non-compliance with this policy can lead to the application of the discipline policy.

Monitoring Activities of HIPAA

One of the ways to evaluate the success of the Corporate Compliance Program is to routinely review and assess the activities and operations of the organization. Comprehensive Systems, Inc. has established an On-Site Review Committee composed of administrative employees who routinely monitor activities within the organization to ensure that employees, contractors and other persons acting on behalf of Comprehensive Systems, Inc. are adhering to the organization's policies and procedures. A form is used to check for HIPAA privacy compliance and to interview staff. An on-going review is completed in all service areas to assess the effectiveness of HIPAA safeguards and employee knowledge. Areas of concern are corrected through staff training, or through minimal structural or environmental changes. Oversight of these activities is a function of the Compliance Committee.

Reporting Concerns of Questionable Conduct

Employees who suspect or know of any violations, or potential violations, of any part of the Corporate Compliance Policy that are of a non-personnel nature are expected to report those violations utilizing the procedures established in the Corporate Compliance Program. The first step of reporting should be to their supervisor. However, if an employee is not comfortable discussing a concern with his or her supervisor, or the employee is not satisfied with his or her supervisor's response, the employee is expected to take the next step. The concern should then be reported to the Corporate Compliance Director, the HIPAA Privacy Officer or to another member of the compliance committee.

Complaints deemed to be of a personnel nature will be investigated by the HR Director following the grievance/complaints procedure outlined in either the General Handbook for Non-Administrative Employees or the Administrative/Professional Employee Handbook.

All reports of a compliance violation will be taken seriously and will be promptly investigated under the direction of the Corporate Compliance Director. To ensure that the Compliance Director has all the information necessary to thoroughly investigate a report, Comprehensive Systems, Inc. strongly encourages direct communication of the concern by an employee to his or her supervisor, to the Corporate Compliance Director, the HIPAA Privacy Officer or to another member of the compliance committee. It should be noted that complaints deemed of a personnel nature, will be referred to personnel services. Following an investigation of a reported concern, the Compliance Director or designee will report back the outcome of the investigation to the employee who made the report.

Comprehensive Systems, Inc. has designed a system to help protect the identity of an employee who reports a compliance concern. Every reasonable effort will be made to keep a reporting employee's identity confidential, but complete protection of privacy will not always be possible. It must be understood that there are no absolute guarantees regarding confidentiality once a corporate compliance "report" is submitted. In addition, there are some circumstances under which Comprehensive Systems, Inc. may be required by law to disclose a reporting employee's identity, such as under a subpoena to produce records or give testimony. Employees may also give permission to Comprehensive Systems, Inc. to reveal their identity.

Any employee who suspects Medicaid waste, abuse or fraud should immediately report the allegation to his/her supervisor or the Corporate Compliance Director or member of the Compliance Committee. A report can also be made to the President of the Board of Directors of Comprehensive Systems, Inc. For those not comfortable with reporting in person, a written and anonymous Confidential Report of Concern may be completed. (f307.1)
An internal investigation will be initiated immediately after a report is received. Appropriate corrective actions will be taken as a result of the investigative findings, including self-reporting to the Department of Human Services (DHS). Suitable disciplinary actions will be implemented as a result of the internal investigation. All founded allegations related to the investigation will be maintained in the Corporate Compliance Director's confidential records.
Employees may also report suspected Medicaid waste, abuse or fraud to:

- Iowa Medicaid Director, Division of Medical Services, Department of Human Services, 100 Army Post Road, Des Moines, Iowa 50305, phone (515) 725-1121, fax (515) 725-1010.
- Iowa Medicaid Fraud Control Unit with the Department of Inspections and Appeals, Lucas State Office Building, 3rd Floor, Des Moines, Iowa, 50319, phone (515) 281-6377, or (800) 831-1394, fax (515) 242-6507.
- Iowa Medicaid Program Integrity, phone (877) 446-3787 or (515)256-4615.
- Health and Human Services Office of Inspector General, phone (800) 447-8477, fax (800) 223-8164, email hhstips@oig.hhs.gov. Mailing address: Office of Inspector General, Department of Health and Human Services, Attn: hotline, 330 Independence Ave. SW Washington DC 20201.

No disciplinary action or retaliation will be taken against an employee who makes a good faith report of a compliance violation. Anyone who retaliates against an employee for reporting a compliance violation will be subject to disciplinary action, up to and including termination.

To further promote reporting of compliance violations, Comprehensive Systems, Inc. has established an anonymous reporting system that permits employees and contractors to report concerns on an anonymous basis. This system has been established for those persons who, for whatever reason, are not comfortable taking their concern to their supervisor, to the Corporate Compliance Director, the HIPAA Privacy Officer or to a member of the Compliance Committee. Just as any other report, a concern reported through the anonymous reporting system will be investigated under the direction of the Corporate Compliance Director. Because the report was made anonymously, the Corporate Compliance Director will not be able to report back the outcome of the investigation to the employee who made the report.

An anonymous report can be made by completing a Confidential Report of Concern Form and mailing it to the Corporate Compliance Director at the designated address. If a report is made anonymously in writing, it must be sufficiently detailed to provide a factual basis for the allegations in order to allow an appropriate investigation. It must be noted that effective investigation and appropriate resolution of reported concerns are made more difficult by anonymous reports. The possibility exists that an investigation may not be able to be completed due to the anonymity of the report. Employees are urged to identify themselves when making any report.

The above notwithstanding, the filing of a false or intentionally inaccurate Confidential Report of Concern through the anonymous reporting system shall be considered a serious offense. The anonymous reporting system is not intended to provide an opportunity for employees or contractors to get other employees "in trouble", but rather is intended solely as a methodology for the reporting of the violations set forth above. The filing of an intentionally false or misleading report could subject an employee to disciplinary action up to and including termination.

Confidential Report of Concern

The purpose of this form is to report the facts pertaining to any known or suspected violation of the Corporate Compliance Policy. Although we ask you to provide your name, it is not necessary for you to do so if you wish to make an anonymous report. An anonymous report can be made by completing this form and mailing it to the Corporate Compliance Director at Comprehensive Systems, Inc. at the following address: P.O. Box 1186, Mason City, Iowa 50402.

If you do not want to give your name, you may call the Corporate Compliance Director after one week of submitting this report to inquire about the status of the investigation. You may be asked detailed questions about the report in order to verify your authenticity. If you do not call, the Corporate Compliance Director will not be able to report back the outcome of the investigation arising out of your report.

If you wish to identify yourself in this report, Comprehensive Systems, Inc. will make every effort to keep your identity confidential. Only the Corporate Compliance Director, and others designated by the Compliance Director to conduct investigations, will have access to your initial report. It must be understood that there are no absolute guarantees regarding confidentiality once a corporate compliance report is submitted. There are some circumstances under which Comprehensive Systems, Inc. may be required by law to disclose a reporting employee’s identity. In addition, employees may also give Comprehensive Systems, Inc. permission to reveal their identity.

Please include all the factual details of the suspected violation, however big or small, to ensure the Corporate Compliance Director has all the information necessary to conduct a thorough investigation. Please attach additional pages as needed. The information you provide should include names, dates, times, places and a detailed description of the occurrence that led you to believe a violation of the principles of the corporate compliance program occurred. Please include a copy or a description of any documents that support your concerns.

False Reports

Filing a false report is a serious offense. Reporting in not intended for petty gripes or to get another employee "in trouble." Any employee, filing an intentionally false or misleading report, would be subjected to disciplinary action up to including termination.

Disciplinary Guidelines

Members of the organization will be subject to disciplinary action for failure to comply with the legal and ethical standards adopted by Comprehensive Systems, Inc. Strict adherence to the organization's policies and procedures is a condition of employment. Violations of the Code of Conduct, the Corporate Compliance Program policies and procedures or departmental policies and procedures will result in disciplinary action, up to and including termination, as determined on a case-by-case basis.

Comprehensive Systems, Inc. generally follows progressive disciplinary steps in determining the disciplinary action or sanctions to be applied against an employee for violation of the organization's policies and procedures. The range of disciplinary action includes oral or written warnings, suspension from employment and termination of employment. These progressive disciplinary steps are used by Comprehensive Systems, Inc. as a guideline, and should not be construed as prohibiting Comprehensive Systems, Inc. from taking other disciplinary action that it feels, in its sole discretion and judgment, is appropriate under the circumstances. Comprehensive Systems, Inc. reserves the right to terminate an employee at any time, for any lawful reason, with or without warning.

Although disciplinary actions may vary according to the nature and severity of the violation, disciplinary actions will be consistently applied and enforced against all levels of employees who commit similar violations under similar circumstances. In general, Comprehensive Systems, Inc. personnel will be subject to disciplinary action for violating the policies and procedures referenced in this program, failing to report a violation of the policies and procedures referenced in this program, failing to cooperate during an investigation of a suspected violation, and failing to take reasonable steps to detect and correct a violation within an employee's area of responsibility.

An employee's legal and ethical conduct contributes to the success of the Corporate Compliance Program, as well as to the success of the employee's job performance. An employee's adherence to the organization's policies and procedures, including the employee's responsibility to report known or suspected violations, will be assessed and recognized as a part of the employee's performance evaluation.

Investigations

The Corporate Compliance Director or HIPAA Privacy Officer will conduct a prompt and confidential investigation in response to a reported violation of the Corporate Compliance Program policies and procedures, or a HIPAA violation. All employees are expected to cooperate fully in an investigation. Failure of an employee to cooperate in any investigation may lead to disciplinary action. Retaliation against any employee who cooperates in an investigation is strictly prohibited and will lead to disciplinary action, up to and including termination. Investigations will be conducted as follows:

If the report of concern or a violation is expressed informally (verbally) at the time of the occurrence by the person who observed the activity in question, or through a subsequent communication with the individual's supervisor, the supervisor shall meet with the individual to discuss and review the allegation. The supervisor will take notes of the discussion and pass those notes on to the Corporate Compliance Director. If possible, informal allegations will be resolved within five (5) business days from when the allegations were made. Such resolution shall be reported to the Compliance Director.

HIPAA violations, along with the outcome of the investigation, and disciplinary measures will be reported to The Office of Inspector General, and a follow-up letter sent to the individual whose privacy was violated, or that individuals' parent or guardian.

If the allegation comes through the formal process of a Confidential Report of Concern, the Compliance Director will be responsible for conducting the appropriate investigation as follows:

a. Review the Confidential Report of Concern and determine what, if any, additional information is required.

b. Within 5 days of receipt of the Confidential Report of Concern, meet with the supervisor of the employee involved to determine the scope of the investigation.

c. Interview the employee involved and review any documents relevant to the allegation.

d. Within 10 business days of receipt of the Confidential Report of Concern, prepare a written report of the investigation and present the report to the Compliance Committee. After reviewing the report of the investigation, the Compliance Committee will either make a recommendation for additional investigation, or submit the Compliance Director's report to the Executive Director and Board President along with a recommendation as to whether the report should be determined to be founded or unfounded.

e. Any founded allegations will be documented in the employee's personnel file along with a record of any disciplinary actions taken as the result of the investigation.

f. Any unfounded allegations will be reviewed and discussed, if possible, with the reporting employee and the individual against whom the allegation was made. All documentation regarding unfounded allegations will be destroyed.

Training Certification

Employees, volunteers and members of the Board of Directors will certify that they have received, read, and been trained in Comprehensive Systems, Inc.'s Corporate Compliance Program at orientation and annually, thereafter. Each will attest to comply with the policies and procedures of the Corporate Compliance Program and understand that a violation of its standards may lead to disciplinary action, up to and including termination of employment and/or appointment to the Board of Directors.

When an employee has fulfilled the above requirements, a certificate designating this completion will be signed by the employee and the trainer, and it will be kept in the employee's personnel file.

When a volunteer has fulfilled the above requirements, a certificate designating this completion will be signed and kept in the volunteer file.

When a member of the Board of Directors has fulfilled the above requirements, a certificate designating this completion will be signed by the board member and the Corporate Compliance.

P0307