Greystone Programs, Inc.

CORPORATE COMPLIANCE GUIDE

Includes:

CODE OF ETHICAL & LEGAL CONDUCT

HIPAA/HIPAA HITECH

MISSION STATEMENT

Greystone Programs is committed to providing exceptional services and life enriching opportunities for children, adults and families living with autism and other developmental disabilities.

Updated December 2015

INTRODUCTION

Greystone Programs, Inc. is committed to fostering a compliant and ethically sound business culture. To this end, Greystone established a Corporate Compliance Program in 2001. This program is designed to incorporate long standing compliance related activities, such as quality improvement, service guidelines, fair labor standards, to name a few, with new initiatives that ensure compliance with risk areas as they are defined by the U.S. Office of Inspector General and other regulatory agencies.

Each and every employee is expected to carry out their daily tasks in a legal and ethical manner that can withstand the scrutiny of others, including outside regulatory agencies. Said differently, all employees are expected to abide by the rules, regulations and policies that govern their job. There are core standards and values that must be upheld for every employee such as interacting with the individuals we serve, vendors and coworkers in an honest and truthful manner. In addition, there are job-based functions that require strict adherence to specific laws, rules, and regulations based on the task performed. For example, a direct support professional has rules unique to his/her function, such as building a working relationship that is genuine, empathic and reflects a partnership for achieving individual's dreams. Whereas the agency's Billing Specialist is not focused on working one on one with an individual, but concentrates on ensuring billing for services in a compliant manner to the appropriate provider.

Please note that in addition to carrying out their work duties in a compliant and ethical manner, employees also are expected to bring forth any suspected compliance issues to their Manager/Department Head, Human Resources, the Corporate Compliance/Privacy Officer or the **Confidential Helpline (845) 452-5772 extension 314**

Understanding that each employee's role in the organization determines the additional rules and regulations that the employee must follow, Greystone Programs, Inc. has structured its compliance program and employee education to focus on the departmental and functional level. The role of the Corporate Compliance/Privacy Officer is to ensure that any overarching issues are addressed and to assess which areas require focused attention at any given time.

The CEO of Greystone has the ultimate authority and responsibility for the implementation of the agency's corporate compliance program. The CEO and/or designee have the authority and responsibility for compliance with laws and regulations and to report misconduct to the appropriate enforcement authority.

In 2001, Greystone began the development of a Corporate Compliance Program. The following foundation for the program was developed:

- Designating the Corporate Compliance/Privacy Officer;
- Establishing the **Confidential Helpline – (845) 452-5772 Ext. 314;**
- Adopting the Code of Ethical and Legal Behavior;
- Developing an introductory training program for all employees;
- Revising policies to include Corporate Compliance;
- Analyzing risk areas within the organization; and,
- Regularly reporting compliance issues to the CEO and the Board of Directors.

Corporate Compliance/Privacy Officer – Duties & Responsibilities:

- Coordinate the Corporate Compliance Program;
- Develop and maintain Compliance related policies and procedures;
- Establish employee reporting channels, including, but not limited to, a compliance helpline, which employees may use to report problems and concerns without fear of retaliation;
- Implement agency-wide training and communication programs to ensure that all employees and affiliated parties are educated on the Code of Ethical and Legal Behavior, the Corporate Compliance Program, and other specific issues deemed necessary;
- Monitor the agency-wide training and communication programs for periodic updates;
- Delegate responsibility to conduct appropriate compliance investigations (i.e. legal, human resources, and internal audit) to ensure proper follow-up and resolution;
- Coordinate and conduct inquiries and/or investigations when deemed necessary;
- Establish audit controls and measurements to ensure correct processes are established;
- Maintain a working knowledge of relevant issues, laws, and regulations through periodicals, seminars, training programs, and peer contact;
- Report quarterly to the Board on the status of the compliance program;
- Respond appropriately if a violation is uncovered, including a direct report to the Chief Executive Officer (CEO), Board of Directors or external Agency if deemed necessary;
- Report directly to the Chief Executive Officer (CEO).

Where to Report/Helpline:

Anyone who suspects a non-compliance issue can report concerns to the following:

- Your Manager/Department Head
- Human Resources
- The Corporate Compliance/Privacy Officer
- Greystone Helpline **- (845) 452-5772 extension 314**

The Helpline is a tool for employees to use to get a compliance question answered or to report a suspected violation of a rule or regulation.

The Helpline number is (845) 452-5772 Ext. 314.

A caller may anonymously report an issue if he/she chooses. Greystone encourages and prefers that callers identify themselves for clarification and investigation purposes. If a caller identifies themselves, whenever possible, every effort will be made to keep their involvement confidential. These calls are taken seriously and Greystone will not allow any retaliation against a caller who makes a good faith report.

The Helpline voicemail box is monitored by the Corporate Compliance/Privacy Officer and is available 24 hours a day, seven days a week. All call reports are logged and reviewed confidentially by the Corporate Compliance/Privacy Officer and an investigation and remediation are initiated, if appropriate.

Corporate Compliance Reporting Process

1. Compliance Violation Identified
2. Report Violation to Manager/Department Head, Human Resources, Corporate Compliance/Privacy Officer or the Helpline
3. Complaint entered into log and assigned a number
4. Corporate Compliance/Privacy Officer notifies CEO
5. Investigation team identified and notified
6. Investigation conducted and findings reported
7. Recommendations for corrective action identified and implemented
8. Corporate Compliance/Privacy Officer responds to person who identified the violation
9. Investigation concluded
10. Ongoing monitoring

Internal Investigations and Corrective Action:

Greystone Programs is committed to investigate all reported violations promptly and confidentially to the extent reasonably possible. The Corporate Compliance/Privacy Officer will coordinate all aspects of the investigation. The Human Resources department will coordinate investigations involving allegations of harassment, sexual or otherwise, employee grievances, suspected violations of ADA, FMLA, EEOC and other discrimination. The Human Resources department will keep the Corporate Compliance/Privacy Officer apprised of the outcome of such investigations. All reportable and serious reportable incidents/abuse will be investigated as per Greystone's policy and dealt with according to Office for People with Developmental Disabilities (OPWDD) and Justice Center regulations. All employees are expected to cooperate to the fullest extent possible with any and all investigations.

Once a compliance investigation has been completed, the reporting self-identified person will be given a brief summary of whether the allegations were substantiated and corrective action taken to the extent possible.

Corrective action plans will be reported to the Greystone Programs Inc. Board President, the CEO and the affected department head. It is the responsibility of the department head to ensure corrective actions are carried out and report back to the Corporate Compliance/Privacy Officer within outlined time frame when the corrective action plan is completed.

Completed reports by the Corporate Compliance/Privacy Officer will be reported directly to the Chief Executive Officer and the Board of Directors.

Disciplinary Action for Violations:

Disciplinary actions, including termination, may be taken for the following:

- Violating the Greystone Programs, Inc. Code of Conduct.
- Failing to report a violation of the Code of Conduct or to cooperate in an investigation.
- Retaliation against an individual for reporting a violation or possible violation.
- Deliberately making a false report of a violation of the Code of Conduct.

Audit and Monitoring:

Regular auditing and monitoring processes ensure compliance with the rules and regulations. Greystone has identified risk areas that should be routinely audited. If changes are needed, the changes are implemented and then monitored to make sure the changes are working.

The Corporate Compliance/Privacy Officer is responsible for overseeing the various monitoring and audit activities. Managers/Department Heads will be asked to provide various reports and audits to the Corporate Compliance/Privacy Officer so that their respective areas of responsibilities can be monitored. Managers/Department Heads will also identify any risk areas. These risk areas will be reviewed and implementation of corrective action will be completed by the Manager/Department Head as directed by the Corporate Compliance Officer/Privacy Officer.

Sanctions Checking for All Employees:

Greystone Programs, because it participates in the Medicare, Medicaid and other federally sponsored healthcare programs, is not allowed to employ, contract with or bill for any services provided by any person who has been suspended or excluded from participating in federal healthcare programs (such as Medicare and Medicaid).

To ensure that Greystone Programs, Inc. is in compliance with this rule, every active employee, consultant, contractor and vendor is checked quarterly against the publicly posted list of suspended or excluded persons. All new staff is checked against the list before hire. (Online at: www.oig.hhs.gov/fraud/exclusions.asp and www.omig.state.ny.us)

Exit Interviews:

Human Resources personnel conduct exit interviews with employees who leave Greystone Programs' employment. The purpose of these interviews is to get feedback on the employee's experience at Greystone Programs and to look for ways to improve work life in the future. As part of the exit interview process, we ask employees if they have witnessed or know about any compliance issues.

Gifts and Gratuities Policy:

Greystone Programs, Inc. has a clear policy on the acceptance of gifts. At no time is an employee to accept cash from vendors or other agency-related persons. In addition, employees may not accept any non-cash gift with a value of $50.00 or more. An employee who receives a non-cash gift of $50.00 or less must report it to their Manager/Department Head. We encourage those who wish to express gratitude to write letters of recognition, make a donation in the employee's name to the agency or send flowers or cookies for use by the agency.

Annual Conflict of Interest Disclosure by Management and Board Members:

All employees have an obligation to conduct business within guidelines that prohibit actual or potential conflicts of interest. A conflict of interest policy was established to ensure that services provided and business activities are conducted in an objective manner and are not motivated by desire for personal or financial gain.

On an annual basis, Greystone Programs distributes the Greystone Conflict of Interest Policy and Disclosure Statement. Every Board Member and executive-level employee must complete the Annual Disclosure Statement, which is then reviewed by the Board's Audit Committee. Any and all real or potential conflicts of interest must be disclosed and reported to the Board of Directors.

False Claims and Whistleblower Protections

Greystone Programs is committed to prompt, complete and accurate billing of all services provided to Individuals. Greystone and its' employees, contractors and agents shall not make or submit any false or misleading statements or entries on any claim forms.

The False Claims Act prohibits fraudulent billing of services for payment through the state or federal Medicaid system. Examples of false claims, or fraudulent billing practices include:

- knowingly presenting (or causing to be presented) a false or fraudulent claim for payment;
- knowingly making, using, or causing to be made or used, a false record or statement material to a false or fraudulent claim;
- knowingly making, using, or causing to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay money or transmit property to the Federal Government.
- conspiring with others to commit a violation of the False Claims Act;

If you have reason to believe that someone is engaging in false billing practices or false documentation of services or has engaged in other misconduct (fraudulent, illegal, dishonest or otherwise inappropriate action or omission of action), you are expected and encouraged to report the practice to our Corporate Compliance Officer.

Any form of retaliation against an employee who reports a perceived problem or concern in good faith is strictly prohibited by the Whistleblower Protection Act.

GREYSTONE PROGRAMS, INC.
CODE OF ETHICAL AND LEGAL CONDUCT

The Code of Ethical and Legal Behavior applies to all employees, volunteers, and consultants. It clearly states that Greystone Programs, Inc. sets high standards and that each person is expected to follow the rules and regulations that apply to their job. In addition, every employee is obligated to report issues of non-compliance. Each employee must report to their Manager/Department Head, Human Resources, the Corporate Compliance/Privacy Officer or the Helpline any suspected violation by employees, vendors or subcontractors of applicable laws, rules, regulations or the Greystone Code of Conduct. The consequence of not following the Code of Ethical and Legal Behavior is discipline up to and including termination.

PURPOSE: Greystone Programs, Inc's Code of Ethical and Legal Behavior guides us in all that we do. It does not replace any of the more specific policies of the agency. Rather, it is intended to support our mission to provide the highest quality services to all those we serve and to continuously seek improvement.

STATEMENT OF COMMITMENT: In all aspects of facility operations, all **employees, volunteers, board members, and consultants** will perform their responsibilities/functions with uncompromising commitment to ethical and legal standards, specifically as they relate to:

- Honesty
- Fairness
- Integrity
- Good faith
- Respect, and
- The law

All decisions will be made in the best interest of the organization and those served by Greystone Programs, Inc. These decisions should be made considering whether the action is right, fair, and legal**,** and whether that action could withstand the scrutiny of outsiders**,** including, but not limited to:

- Individuals and their families
- Employees
- Physicians and other providers
- Vendors
- Payers
- Community agencies
- Regulatory agencies, and
- The community as a whole

Maintaining integrity and high ethical/legal standards requires hard work, courage, and difficult choices. Each individual must accept responsibility for compliance with this code. Commitment to these standards should never be compromised for financial, professional, or other business purposes.

COMPLIANCE WITH THE CODE OF ETHICAL AND LEGAL CONDUCT:

All staff, volunteers and consultants are expected to comply with this code. The following standards provide definitive expectations and examples of **unacceptable** behavior.

STANDARDS:

1. **Disclose Potential Conflicts of Interest.** Conflict of interest occurs in situations where a person has the potential to direct or influence a decision to his/her own gain.

EXAMPLES:

- Accepting gifts of significant value that could influence one's work-related decision-making, including providing preferential treatment.
- Using business information resources for personal gain or profit.

2. **Adhere to all Agency Policies and Procedures.** Agency policies and procedures were developed to ensure equality, fairness and safety for all employees, as well as to ensure the proper functioning of the Agency.

EXAMPLES:

- Creating a harassing work environment; not complying with anti-discrimination laws.
- Reporting to work under the influence of alcohol or illegal drugs.

3. **Maintain Accurate Documentation, Billing, Coding, and Reporting Procedures and Practices, both operational and financial.** Data integrity and accuracy, as well as retention are critical for support of the individuals we serve and regulatory compliance. The Agency will only bill and accept revenues for which it is entitled.

EXAMPLES:

- Billing for an individual for days he/she did not receive Community Habilitation at home or in an IRA.
- Billing and receiving funds for a quality of service which is lower than that which we are expected to provide.
- Falsifying records including signatures and dates.

4. **Understand and Adhere to the Individual Bill of Rights.** The Individual's Bill of Rights sets forth the minimum guidelines for ensuring that no individual shall be deprived of any civil or legal right solely because of a diagnosis of developmental disability.

EXAMPLES:

- Providing differential care due to race, religion, sexual orientation, etc.
- Not maintaining confidentiality with regards to all information contained in the individual's records.
- Not providing individuals with a balanced and nutritious diet, served at appropriate times and in as normal a manner as possible.
- Not providing privacy of individuals in all aspects of personal hygiene.

5. **Represent the Agency in a Fair and Honest Manner in all interactions.**

EXAMPLES:

- Offering illegal inducements for referrals to the Agency.
- Misrepresenting Agency services and functions.
- Altering Agency documentation.

6. **Safeguard Greystone Assets.** Greystone resources are to be used for job related purposes and not for personal gain.

EXAMPLES:

- Falsifying time sheets.
- Stealing Agency equipment/supplies.
- Using Agency property such as vehicles, fuel cards, computers/internet access, office supplies, etc. for personal use.
- Consuming food meant for the individuals served by Greystone.

7. **Work in a manner that supports the Greystone Vision/Mission and Values Statements (and supports a work environment in which everyone involved is comfortable).** Assume responsibility and accountability for your actions and decisions. Actively seek advice and guidance on ethical issues from others as needed when making decisions. Avoid placing blame and admit mistakes.

EXAMPLES:

- Calling in sick when you are not sick.
- Misrepresentations of individuals or co-workers.
- Acting in any way that creates a hostile work environment for your colleagues.
- Engaging in gossip in the workplace.

8. **Comply with all Applicable Laws, Regulations, Codes, and Policies (including State and Federal Laws).**
Each employee will be made aware of the specific issues affecting his/her area and is responsible for adhering to laws relating to environmental, personal property, business specific, professional licensure/registrations/codes of conduct.

EXAMPLES:

- Committing an unlawful act on facility premises.
- Not renewing or maintaining good standing with your professional licensure or certification.

9. **Be Good Stewards of the Community's Trust.** As a community human services agency, the resources entrusted to us are to be used for the benefit of the community and fiduciary decisions are to be made in the best interest of the community.

EXAMPLES:

- Being wasteful/not being cost conscious.
- Not considering community need when planning new programs.

10. **Uphold the Code of Ethics Relative Human Service Professionals.**
Many positions such as Direct Support Professionals, Nurses and Social Workers have their own Code of Ethics related to that particular profession. We will be aware of, familiar with and use these codes in our employment at Greystone Programs, Inc.

11. **Protect the Confidentiality of Staff, Individuals served and Agency Sensitive Information.** All Greystone representatives and employees are responsible to safeguard and respect the confidentiality and privacy of the individuals we support in accordance with the rules and regulations of HIPAA and HIPAA HITECH.

EXAMPLES:

- Not maintaining confidentiality during an investigation.
- Inappropriately releasing information regarding an individual we serve.
- Looking up an individual's diagnosis or test result without consent.
- Disclosing the names of individuals served outside of the workplace.

Any questions, comments, or concerns regarding this Code may be brought to your Manager/Department Head or the Corporate Compliance/Privacy Officer.

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT (HIPAA)

PURPOSE:
Greystone is committed to maintaining the privacy of all staff and individuals served and seeks to ensure the confidentiality of all information about them. Protected health information is strictly confidential and should never be given, nor confirmed to anyone who is not authorized under the Agency's policies or applicable law.

HIPAA is a federal regulation that gives widespread protection over the privacy of a person's confidential protected health information. This law became effective August 21, 1996. The law has three components: Privacy, Security and Electronic Data Transmission of individually identifiable patient health information. The U.S. Department of Health and Human Services (HHS) is the monitoring agency. (Refer to Health Insurance Portability and Accountability Act Privacy Policy-HIPAA:03 and HIPAA:01)

PROTECTED HEALTH INFORMATION (PHI) DEFINED:
For the purposes of this policy, the term protected health information (PHI) means any individual information, including very basic information such as their name or their address, that **(1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.**

Some examples are:

a. Health condition and health care benefits;
b. Demographic information (name, address, race, gender, ethnicity or marital status);
c. Social security number, medical record number, driver's license number, full face photos; or
d. Other types of information that may identify who the individual is.

In compliance with HIPAA we will maintain the privacy of all staff and individuals we serve by protecting their confidential identifiable health information in any form, including spoken, written or electronic form.

All information accessed concerning all individuals and staff as part of their daily work should be discussed only in work settings, on a need-to-know basis, not in public areas and only when it is appropriate. Any discussion about someone's confidential information when it is not necessary or outside of the workplace is prohibited. All discussions and conversations should be professional and maintain a level of integrity that respects your co-workers and individuals you serve. Employees will not discuss any person's record with unauthorized associates, whether on or off duty. (Refer to Confidentiality of Protected Health Information Policy-HIPAA:01)

Staff should be careful not to discuss an individual who receives services while in the presence of other individuals. Employees should be mindful as to the presence of all other individuals before engaging in a discussion regarding a person receiving services.

Employees must limit information shared in a discussion with an individual's personal representative/family member to facts that relate to that individual's care or payment for the care. The divulging of information relating to other individuals is prohibited.

All files containing PHI should be kept in a confidential location where only authorized staff is allowed access. Offices, workstations, computers, file cabinets, fax machines and all other areas that may contain PHI must be kept secured at all times. Only people with need-to-know responsibility can have access.

WHEN ARE YOU ALLOWED TO DISLOSE PROTECTED HEALTH INFORMATION?

All Greystone Programs staff is generally expected to limit their uses and disclosures of Protected Health Information (PHI) and requests for protected health information, to the minimum amount of information necessary to perform their duties for the Agency. This expectation does not mean that we are restricting exchanges of information required in order to serve individuals and staff quickly and effectively.

Under the privacy regulations of HIPAA, an individual receiving services has the right to request and accounting of whom Greystone Programs, Inc. has shared their confidential information with. Each individual's General, Nursing and Medicaid Service Coordinator file has a PHI Disclosure Log in the front of the file. Every person who reviews any information in the file needs to sign in on the disclosure log; this includes internal and external people.

All other disclosures require a signed *Authorization to Disclose Form* from the individual whose protected health information (PHI) you are being asked to disclose. If a particular situation does not allow you to use, disclose or request protected health information in a way that you believe is necessary to carry out your duties, you should notify your supervisor.

As a member of our staff, you will routinely use protected health information regarding individuals to carry out your duties. You may also need to disclose protected health information about individuals or staff to persons outside or within the agency who request protected health information about these persons.

Each department will, according to business necessity, designate who will have access to protected health information and how that information will be disclosed. (Refer to Minimum Necessary Standard in Routine Situations Policy-HIPAA:02) Generally, Protected Health Information (PHI) is unrestricted if it is necessary to disclose for the purposes of **providing treatment, payment or operation of services**.

The minimum necessary rule does not apply to:

a. Disclosures to or requests by a health care provider for treatment purposes
b. Disclosures to the individual who is the subject of the information
c. Uses or disclosures made pursuant to an authorization requested by the individual
d. Uses or disclosures required by compliance with the standardized HIPAA electronic transactions
e. Disclosures to the Department of Health and Human Services (HHS) when required for enforcement purposes.
f. Uses or disclosures that are required by other law

Electronic Business Communication & HIPAA HITECH:

(Refer to Business Communications Policy-HIPAA:04)

For privacy reasons, employees should not attempt to gain access to another employee's personal e-mail file or voice mail messages without written permission. Employees should anticipate that an e-mail or voice mail message might be disclosed to or read by individuals other than the intended recipient(s), since messages can be easily forwarded to other individuals. In addition, while Greystone Programs, Inc. strives to maintain the reliability of these systems, employees should be aware that a variety of human and system errors have the potential to cause accidental disclosures of e-mail messages.

Computer and voice mail passwords are intended to keep unauthorized individuals from accessing messages stored on the systems. Employees are expected to ensure that they exit any confidential database upon leaving their workstations so that protected health information (PHI) is not viewed by unauthorized members. The failure to keep passwords confidential can allow unauthorized individuals to gain access to confidential items as well as read, modify, or manipulate files on other systems. (Refer to Information Technology Security Policy-HIPAA:08).

Employees should not download, copy or remove from the agency any protected health information, except as necessary to perform their duties at Greystone. Upon termination of employment or contract with Greystone, or upon termination of authorization to access PHI, members must return to Greystone any and all copies of PHI in their possession or under their control.

Employees should not transmit PHI over the internet or other unsecured network unless using secure encryption procedure. Transmission of PHI is permitted by fax only if the member sending the information ensures that the intended recipient is available to receive the fax as it arrives, or confirms that there is a dedicated fax machine that is monitored for transmission of sensitive information. A cover sheet that includes standard confidentiality notices and request that the recipient call the staff member upon receipt of the fax must be used.

Members of this agency who violate these policies will be subject to disciplinary action up to and including termination of employment or contract. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his/her Manager/Department Head or the Privacy Officer.

Protocols for Responding to an Investigation by a Governmental Agency:

Multiple government agencies are responsible for health care corporate compliance. They can include the FBI, Department of Health, IRS, state and local police, OPWDD, Justice Center, Office of the Medicaid Inspector General, to name a few. Greystone Programs has established formal protocols so that in the event that a government agency presents at an agency site/program and request information, staff and management are prepared.

Greystone responds in a proper manner to all government investigations. Some of the governmental entities that have a right to immediate access to information are:

- New York State Office for People with Developmental Disabilities (OPWDD)
- New York State Office of the Attorney General (NYS AG)
- New York State Department of Health (NYS DOH)
- New York State Fraud Control Unit
- New York State Department of Labor (NYS DOL)
- United States Department of Health and Human Services (HHS)
- United States Occupational Safety and Health Administration (OSHA)
- Health Care Financing Administration (a division of HHS)
- United States Office of Inspector General (OIG)
- Mental Health Legal Services (MHLS)
- New York State Commission of Quality Care(NYS CQC)
- New York State Office of Mental Health (NYS OMH)
- Office of Children and Family Services (OCFS)
- NY State Department of Education

Staff Protocol for Responding to Government Agency Request for Information:

1. Confirm the identity of the person requesting the information by asking to see an ID badge. Be polite and courteous and ask the nature of the visit.

   Multiple agencies are responsible for corporate compliance investigations. Agents/Agency personnel carry identification badges. All personnel are required to provide their identification when requested.

2. Immediately notify your Manager/Department Head of the presence of agency personnel. If you are asked questions, be aware that you have the right to request the presence of your supervisor and/or an attorney.

3. If your Manager/Department Head is not available, notify the Corporate Compliance/Privacy Officer immediately by calling (845) 452-5772 x314, or notify Human Resources or the CEO.

4. If an agency requests documents/records, refer them to your Manager/Department Head. Non-management staff is not allowed to release documents/records.

Note: Under no circumstance should an employee destroy records or misrepresent facts.

Management & Supervisory Protocol for Responding to Government Agency Requests for Information:

In the absence of an established policy for responding to routine requests for information (i.e. subpoena for medical records, summons from the Department of Health), the following procedure must be followed:

a. Verify that representative is from said agency – request identification and call the agency that they represent.
b. Attempt to determine the reason for the visit, the nature and scope of the request. Request a reasonable amount of time to respond.
c. Immediately notify Corporate Compliance/Privacy Officer, or notify Human Resources or the CEO.
d. Offer a seat in a waiting area away from the flow of normal traffic for your department.
e. Await direction from the Compliance Office and/or legal counsel.

Note: Under no circumstance should an employee destroy records or misrepresent facts. Do not release any documents/records without making a copy and documenting precisely what was released.

SUMMARY:
Compliance is not a department, it is guiding principle factored into each and every decision that we make. Acting in an ethical and compliant manner is each and every employee's responsibility. By adhering to Greystone Programs, Inc. Code of Ethical & Legal Behavior, we can ensure that we are acting in the best interest of the agency, our individuals, co-workers, and our industry.

Acknowledgement

I certify that I have received the Greystone Programs, Inc. Corporate Compliance Guide which contains detailed policies and procedures for recognizing and reporting violations; the agency's Code of Ethical & Legal Conduct, a description of the False Claims Act and Whistleblower Protection Act, HIPAA and HIPAA HITECH training.

I recognize that these documents represent mandatory policies of the Agency and agree to read and abide by them.

_____

Print Name Date

_____

Signature

_____

Work Location/Department