# Annual Compliance Requirements

This packet consists of acknowledgements and signature pages which should be obtained by the facility from all staff on an annual basis. The policies related to each acknowledgment are listed in the Table of Contents and can be found in the CCG Portal.

# Annual Compliance Requirements Table of Contents

# ACKNOWLEDGEMENT OF CODE OF CONDUCT AND COMPLIANCE AND ETHICS PLAN

I hereby acknowledge that I received a copy of the Facility's Code of Conduct, Corporate Compliance and Ethics Plan, and compliance and ethics program policies and procedures and that I had the opportunity to review them. I understand that I should report any compliance and/or ethics concerns to either the compliance and ethics officer of any other member of the Governing Body. I hereby agree to abide by the requirements of this Code of Conduct, the Compliance and Ethics Plan, the compliance and ethics policies and procedures, and the compliance and ethics program in general. I further understand that adherence to this policy is a condition of my continued business dealings with the Facility.

| | |
|---|---|
| _____ | _____ |
| Print Name | Signature |
| _____ | _____ |
| Company Name (If Contractor) | Date |

## Acknowledgement of Training and Receipt of Deficit Reduction Act of 2005 Policy and Procedure

I hereby acknowledge by my signature that I have received and read the Deficit Reduction Act of 2005 Policy and Procedure, agree to comply with it, and understand that:

- This Facility is committed to providing quality care for its residents and submitting reimbursement claims for healthcare services that have been properly provided and that are supported by complete documentation.
- This Facility has a Compliance and Ethics Program that provides support to each employee while providing quality care and adhering to all applicable laws and regulations. I have received a copy of this Facility's Compliance and Ethics Program Manual and I am aware that additional copies are available through the Facility's Administrator or Compliance and Ethics Officer.
- If I have any concerns that may involve a violation of a law or regulation, even if I am unsure if the issue is a violation of any law or regulation, I am encouraged and expected to report such concern without delay.
- Concerns related to this policy may be reported to my manager, the Administrator, or the Compliance and Ethics Officer. Calls may also be made anonymously to the Compliance and Ethics Hotline at **(800) 610-2544**.
- I understand that this Facility will not intimidate me from reporting, nor will I face any retaliation, provided my report was made in good faith.
- This Facility is committed to complying with the Deficit Reduction Act of 2005 as outlined in this Policy and Procedure.
- Vendors and Contractors only: I agree to abide by the standards contained in this Policy and Procedure, and also agree to participate in this Facility's mandatory compliance and ethics training as applicable. I agree to disseminate this Facility's policies to my managers and employees.

_____

Name of individual (Please print)

_____

Name of company (Please print)

Choose one:

❍ Employee

❍ Health Care Provider

❍ Vendor

❍ Other: _____

## ACKNOWLEDGEMENT OF RECEIPT OF AND TRAINING IN PREVENTION OF FRAUD, WASTE, AND ABUSE POLICIES AND PROCEDURES

I hereby acknowledge that the Facility has provided me with copy of the Facility's Fraud, Waste, and Abuse ("FWA") Policies and Procedures that I have reviewed. I further acknowledge that the Facility has provided me with FWA training in the form of the CMS provided FWA training. I am aware that I must report any compliance and ethics concerns to either my manager, the Administrator, the Compliance and Ethics Officer _____, or as a last resort by calling our Compliance and Ethics Hotline at (800) 610-2544. I hereby agree to abide by the requirements of the FWA Policies and Procedures.

_____ _____

Print Name Signature

_____

Date

**** Training must be completed within 30 days of initial hiring and annually thereafter.***

## ACKNOWLEDGEMENT OF RECEIPT OF AND TRAINING IN OVERPAYMENT SELF-DISCLOSURE POLICY AND PROCEDURE

I hereby acknowledge that I have received a copy of the Facility's Overpayment Self-Disclosure Policy and Procedure, and that I must report any compliance and ethics concerns to either my manager, the Administrator, the Compliance and Ethics Officer _____, or as a last resort by calling our Compliance and Ethics Hotline at (800) 610-2544. I hereby agree to abide by the requirements of this Overpayment Self-Disclosure Policy and Procedure.

_____ _____

Print Name Signature

_____

Date

**ANNUAL CONFLICTS OF INTEREST**
**DISCLOSURE STATEMENT**

**Name**: _____

**Date**: _____

**Position**: _____

## Conflict of Interest Policy

The Facility's Conflict of Interest Policy requires each executive employee and contractor in a position to influence the Facility's decision making regarding contracts to disclose annually his or her affiliations and to execute an acknowledgement confirming that he or she has complied with the Facility's Code of Conduct.

Disclosure of an executive employee and contractor's affiliations is intended to assist the Facility in resolving conflicts of interest. An affiliation with another organization does not necessarily mean that an unacceptable conflict of interest exists or that the affiliation would unduly influence the executive employee or contractor.

## Instructions

Please answer all of the questions in Section 3 to the best of your knowledge. If you answer "yes" to any question on this form, please respond fully to the information requested or identify whether the position or relationship is compensated, involves equity (i.e. stock, or other beneficial ownership interest), or involves another financial interest. Use additional sheets if necessary to fully answer any question.

## DISCLOSURE STATEMENT

1. Do you or, to your knowledge, any member of your family have any interest in any entity which conducts business with the Facility?

_____No _____Yes If yes, please explain

_____

_____

_____

_____

2. Do you or, to your knowledge, any member of your family hold any position as a director, officer, partner, trustee, employee, agent or consultant of any entity which conducts business with the Facility?

_____No _____Yes If yes, please explain

_____

_____

_____

_____

3. Have you or, to your knowledge, any member of your family given, directly or indirectly, any gift, entertainment, compensation, reward, or other benefit during the past twelve (12) months to any entity which conducts business with the Facility?

_____No _____Yes If yes, please explain

_____

_____

_____

_____

4. Have you or, to your knowledge, any member of your family received, directly or indirectly, any gift, entertainment, compensation, reward, or other benefit of more than nominal value during the past twelve (12) months from any entity which conducts business with the Facility?

_____No _____Yes If yes, please explain

_____

_____

_____

_____

5. Are you a member of the governing body or an officer, trustee, employee, agent, or consultant of, any other healthcare provider or supplier other than the Facility?

_____No _____Yes If yes, please explain

_____

_____

_____

_____

6. Please indicate whether you are currently debarred, suspended, excluded, or otherwise ineligible to participate in any federal program.

_____No, I am NOT currently debarred, suspended, excluded, or otherwise ineligible to participate in any federal program

_____Yes, I am currently debarred, suspended, excluded, or otherwise ineligible to participate in any federal program. Please provide details of debarment, suspension, or exclusion.

_____

_____

_____

_____

7. Please indicate whether you have ever been convicted of a criminal offense related to the provision of health care items or services.

_____No, I have never been convicted of a criminal offense related to the provision of health care items or services.

_____Yes, I have been convicted of the following criminal offense related to the provision of health care items or services. Please explain and include the offense, date of conviction, and state where offense occurred.

_____

_____

_____

_____

8. Please indicate whether you have entered into or been a party to any agreement or settlement with any governmental body or agency relating to an allegation of non-compliance with, or violation of, any healthcare laws.

_____No _____Yes If yes, please explain the nature of the settlement and include the violation, date of settlement, and state where the violation occurred

_____

_____

_____

Please indicate your knowledge of whether or not the Facility is currently noncompliant with any applicable healthcare laws or regulations or under investigation, audit, or review for any alleged noncompliance with healthcare laws.

_____No, I have NO knowledge of any non-compliance with applicable healthcare laws by the Facility, or knowledge of any investigation, audit, or review of alleged noncompliance with healthcare laws by the Facility.

_____Yes, I am aware of and have knowledge of noncompliance with healthcare laws by the Facility, or I have knowledge of an investigation, audit, or review of alleged noncompliance with healthcare laws. Please explain, in detail, what you have knowledge of by providing a complete explanation and all relevant facts and circumstances.

_____

_____

_____

_____

# Acknowledgement

I hereby certify that I have carefully read and understand all of instructions, questions and disclosures in this Annual Disclosure Statement. I agree to immediately update the information provided in this Annual Disclosure Statement in writing to the Facility Compliance and Ethics Officer in the event of any changes.

I further certify that the information contained on this form is true and correct to the best of my knowledge and I have made reasonable efforts to assure that accurate and complete information has been provided.

Additionally, I certify that it is my responsibility to read, understand and abide by the Facility Code of Conduct and agree to comply with my obligations under the Code of Conduct.

**Signature**:_____**Date**:_____

# ACKNOWLEDGEMENT OF RECEIPT OF POLICY AND PROCEDURE REGARDING RESIDENT FREEDOM FROM ABUSE, NEGLECT, AND EXPLOITATION AND THE ELDER JUSTICE ACT

I hereby acknowledge by my signature that I have received a copy of the Facility's policies and procedures. I hereby agree to abide by the requirements of these policies as well the compliance and ethics program in general. I further understand that adherence to these policies is a condition of employment or continued business dealings with the Facility, and that I have a duty to report any compliance and/or ethics concerns to either my manager, the Administrator, the Compliance and Ethics Officer _____, or as a last resort by openly or anonymously calling our Compliance and Ethics Hotline at (800) 610-2544.

_____ _____

Print Name Signature

_____ _____

Company Name (If Contractor) Date

# Compliance and Ethics Training and Education/ Basics of the Compliance and Ethics Program

I. Per federal and state requirements, this facility has a mandatory compliance and ethics program which is applicable to and any and all owners, directors, officers, clinical staff, employees, independent contractors, consultants, and others ("Associates"). The compliance and ethics program is designed to:

1. Ensure Associates' compliance with all federal and state laws, rules and regulations;
2. Help Associates understand and meet the legal and ethical standards expected by the facility;
3. Emphasize the facility's commitment to accurate and lawful documentation and submission of all claims for services to Medicare, Medicaid, and other third-party payors;
4. Promote the prevention, detection and resolution of any acts that do not conform to applicable federal and/or state laws, rules, and regulations;
5. Minimize, through early detection and reporting, any potential loss to the government from erroneous claims; and to
6. Provide for seamless interaction and communication between the governing board and staff, which helps in correcting any compliance and/or ethics issues and in keeping the facility in compliance with all applicable federal and states statutes and regulations.

II. The Compliance and Ethics Program consists of the following eight elements.

**1. Compliance and Ethics Officer**

A. The Compliance and Ethics Officer is an employee of the facility who handles the responsibility of managing the day-to-day operation of the compliance and ethics program. This facility's Compliance and Ethics Officer is _____. The Compliance and Ethics Officer interacts with, and communicates compliance-related matters to, the governing board through periodic written and/or verbal communications and reports.

**2. Policies and Procedures**

A. The facility has policies and procedures which are accessible to all Associates that are designed to ensure the facility's commitment to compliance and ethics by, among other things, describing compliance and ethics expectations for Associates, and establishing protocols to be followed prior to an occurrence of non-compliance. Examples of policies and procedures are those that address:

a. the implementation of the compliance and ethics program;
b. training and education for all Associates on the compliance and ethics program and potential compliance and ethics issues as part of the orientation process and at least annually thereafter;
c. the facility's commitment of quality of care;
d. the prohibition against retaliation and intimidation for reporting compliance and/or ethics concerns;
e. the prohibition on unlawful harassment and discrimination;
f. the requirement for all Associates to report fraud, waste and abuse;
g. how to deal with compliance and/or ethics issues as they come up;
h. how to properly investigate and resolve compliance and/or ethics issues;
i. the information contained in this training document.

**3. Education/Training of Associates**

A. The facility, as required, provides new orientation and annual compliance and ethics training to all Associates in the form of this training document. All Associates should be aware of the following:

a. The facility has a Corporate Compliance and Ethics Plan, Code of Conduct, and other policies and procedures that implement the compliance and ethics program through an adoption and resolution, describe the facility's compliance and ethics expectations for Associates, and which provide detailed guidance on dealing with compliance and/or ethics issues. Specifically:

i. Associates have a duty to report any questionable conduct, questionable practices, and actual or suspected violations of the compliance and ethics program to their supervisor, the compliance and ethics officer, or the compliance and ethics hotline. When a reporter requests confidentiality, the report will be provided solely to the compliance and ethics officer or his/her designee(s).

ii. Potential compliance and/or ethics problems are investigated and resolved. The Compliance and Ethics Officer will initiate investigations to ascertain if an allegation of non-compliance received through a compliance and ethics reporting channel represents a possible violation of applicable laws, rules, regulations or the compliance and ethics program. The extent of the investigation will vary depending upon the nature of the concern. The facility will take necessary remedial action to the extent it is warranted. The compliance and ethics officer will develop a remediation plan on a case-by-case basis when a compliance and/or ethics violation is detected. The plan will be designed to prevent a recurrence of the violation and is a key factor in evaluating the success of the overall compliance and ethics program. Associates are expected to fully cooperate with and assist the facility in the resolution of reported compliance and/or ethics issues.

iii. The facility expects all Associates at all times (1) to act in a way that meets the requirements of the mandatory compliance and ethics program laws and regulations, and (2) to conduct business in a manner that supports the facility's integrity in operations.

**4. Reporting/Communication of suspected non-compliance**

A. All Associates must report any identified potential compliance and/or ethic other issues as they arise. Reports can be made to an Associate's direct department head, any department head, the compliance and ethics officer directly, or via the CCG hotline (800-610-2544). The hotline number is posted throughout the facility and calls can be anonymous and confidential. Any Associate receiving any such report is required to report such issues to the appropriate compliance and ethics personnel, such as the compliance and ethics officer or his/her designee(s). An Associate who fails to promptly report any such activity will be subject to disciplinary action, which may include termination of employment or contract.

B. If a reporter requests confidentiality, the report will be provided solely to the Compliance and Ethics Officer or his/her designee(s), and confidentiality shall be maintained unless the matter is turned over to law enforcement or disclosure is required during a legal proceeding.

C. The facility has a zero-tolerance policy for intimidation, retaliation, or retribution against any Associate who, in good faith, reports suspected non-compliance, misconduct, or fraud, waste, and abuse by any Associate. All forms of unlawful retaliation are prohibited, including any form of discipline, reprisal, intimidation, or other form of retaliation taken against an Associate for participation in any activity protected by law.

D. Both the law and facility policy protect whistleblowers.

**5. Discipline**

A. The facility has policies and procedures that outline disciplinary standards that are fairly and firmly enforced. Disciplinary action shall be administered on a fair and equitable basis, appropriate to the seriousness of the violation and consistent with the facility's policies and procedures. Enforcement of disciplinary action will be consistent across all levels and rankings within the facility. Depending on the severity of the violation, progressive steps in the disciplinary action process may be omitted in order that immediate corrective measures, including termination, can be taken. The disciplinary policies are used encourage and facilitate the reporting of non-compliant behavior, and to fairly and consistently deal with compliance and/or ethics violations, which includes non-reporting of compliance and/or ethics issues by applicable Associates. Associates who (1) participate in non-compliant behavior; (2) encourage, direct, facilitate, or permit non-compliant behavior; (3) or do not report suspected compliance and/or ethics violations shall be subject to disciplinary measures ranging from an oral reprimand to termination of employment or relationship.

B. Associates are expected to assist, as appropriate, in the resolution of compliance and/or ethics issues.

**6. Auditing and Monitoring**

A. In order to evaluate its program and identify potential compliance and/or ethics issues and to self-evaluate identified risk areas, the facility conducts periodic reviews and external and/or internal audits. The facility also continuously monitors internal processes to ensure the proper identification of compliance and ethics risk areas to enable proper monitoring of potential compliance and ethics issues.

**7. Responding to detected offenses**

A. The facility has a mechanism to respond to potential compliance and ethics issues, which is outlined in the facility's written policies and procedures. Specifically:

a. the facility has a system in effect (1) for responding to compliance and ethics issues as identified in the course of audits and self-evaluations through investigations and corrective actions to ensure that compliance and ethics issues are resolved promptly and thoroughly; (2) for reducing the potential for the recurrence of compliance and ethics issues through proper training, education, and disciplinary actions; (3) for identifying and reporting compliance and ethics issues to the Department of Health and other state agencies; (4) for refunding Medicaid/Medicare overpayments; and (5) for responding to compliance and ethics issues as they are raised through investigations and remedial actions.

**8. Reassessment**

A. The facility will periodically reassess the compliance and ethics program to evaluate its effectiveness and to make any necessary adjustments.

***By signing below, I acknowledge that I have received, read, and understood the materials covered in this training. I have had the opportunity to ask questions and receive responses related to the content of this training, and I understand that active participation in the compliance and ethics program is mandatory.***

_____
Print Name:

_____
Signature:

_____
Date:



2623 Hooper Avenue, Brick, NJ 08723 | Phone (718) 408-8989 | Fax (718) 650-6044 | Info@ComplianceCG.com | www.ComplianceCG.com

1. **Introduction**
   - **a.** The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as Protected Health Information (PHI).
   - **b.** In 2009, HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health). In January of 2013, the Department of Health and Human Services issued a final rule ("Final Rule"), also known as the Omnibus Rule, implementing HITECH's statutory amendments to HIPAA. These latest updates improved patient privacy protections, gave individuals new rights to their health information, and strengthened the government's ability to enforce the law. As technology changes, and covered entities and their associated Business Associates implement new systems, the Omnibus Rule accounts for, and keeps pace with, these advancements and developments.
   - **c.** In general, HIPAA violations are enforced by the Department of Health and Human Services (HHS) Office of Civil Rights (OCR). However, pursuant to HITECH, state attorneys general are also permitted to bring civil actions and recover monetary awards that may be shared with harmed individuals.
   - **d.** Facilities that are subject to HIPAA regulations are called "covered entities" (CEs). Nursing homes, ALF's, other healthcare providers, insurance companies and hospitals are examples of covered entities. (There is no section of the Rule which is *specific* to any specific type of entity.) In addition to maintaining and enforcing the protection of its PHI, CE's are also required to execute written Business Associate Agreements (BAA's) with certain organizations and non-workforce individuals with whom they share Protected Health Information (PHI). Business Associates are outside organizations or non-workforce individuals who perform some function or service, *outside* of providing medical care or treatment, for the CE that makes them likely to have access to PHI (e.g. shredding services, computer hardware/software vendors, third-party billing vendors, etc.) Failure to have compliant BAA's can and has led to civil penalties of tens of thousands up to several million, dollars.
2. **What is Protected Health Information (PHI)**
   - **a.** PHI is defined as:
     - i. Any information that can be used to identify a resident – whether living or deceased – that relates to the resident's past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.
   - **b.** The following categories are examples of PHI:
     - i. Resident names
     - ii. Addresses
     - iii. Telephone numbers
     - iv. Account, record or Social Security numbers
     - v. Dates such as date of birth or date of death
     - vi. Full face photographs or images
     - vii. Any other information, number, code, or characteristic that can be linked to an individual.
   - **c.** Medium – Identifiable patient information is considered to be PHI in any format – verbal, written, or electronic.
     - i. PHI maintained in an electronic form is called e-PHI.
3. **Allowable Uses**
   - **a.** Facilities are allowed to use or view PHI for three purposes: Treatment, Payment, Operations (TPO).
     - i. Treatment – Facilities can access PHI for the care and treatment of a resident.
     - ii. Payment – Facilities can access PHI in order to get paid for treating the resident.
     - iii. Operations – Facilities can access PHI for certain administrative operations, such as Quality Assurance/Quality Improvement activities.
     - iv. Certain DOH or other legally allowed requests.
   - **b.** Individuals may access PHI only for permitted, work-specific purposes.
     - i. Minimum Necessary guidelines prohibit access (including viewing or using) to PHI for non-permissible reasons. Minimum necessary guidelines may result in an individual being allowed to access only certain sections of a medical record.
   - **c.** Incidental use, or minor disclosures of PHI in the process of an allowable TPO use, is acceptable.
     - i. An example of incidental use is the posting of resident names outside resident rooms.
   - **d.** Proper authorization from each patient is required to disclose PHI for most non-TPO activities. The authorization must be clear as to any limitations on the level of disclosure and must include a statement that the individual may revoke their permission at any time of their choosing, among other required elements. When an authorization is needed, a standardized form should be used.
4. **Social Media**
   - **a.** Although there may be *general* benefit to healthcare organizations to use social media to attract new clients and interact with their current patients, it is important to be aware of the considerable potential for violating HIPAA Rules and patient privacy on these networks. It is critical to <u>never</u> disclose unauthorized PHI on social media. Once posted, the digital trail can never be controlled by the original poster.
   - **b.** Social media channels can be used for posting health tips, details of events, new medical research, bios of staff, and for marketing messages, provided <u>no</u> PHI is included in the posts. Sharing images or videos has in many cases determined to be considered abuse and has, in some cases, even resulted in jail time on top of heavy fines. Do <u>not</u> assume that what you might consider innocent/casual sharing activity will be determined as such by an authority. No one can guarantee that a complaint will not be filed. There should be a facility policy in place with respect to executing a proper authorization which will determine what PHI may be shared and where it may be posted.
   - **c.** Resident PHI may never be posted on a staff member's personal social media account.
5. **Unauthorized Access**
   - **a.** It is <u>never acceptable</u> for an employee to look at PHI for non-TPO purposes, even if no harm is intended (e.g., retrieving an address to send a 'Get Well' card).
   - **b.** Unauthorized access to PHI is illegal and against company policy, regardless if the information relates to a "high profile" person or a close friend or family member – ALL information is entitled to the same protection and must be kept private.
   - **c.** HIPAA regulations and PHI restrictions apply to <u>all</u> employees.
   - **d.** Be aware that accessing PHI of someone involved in a divorce, separation, break-up, or custody dispute may be an indication of intent to use information for personal advantage. If you are accessing this information for a legitimate TPO purpose, you may want to review minimum necessary documentation guidelines with your supervisor or your facility's HIPAA Privacy Officer.
   - **e.** <u>Using PHI for personal benefit is prohibited.</u>

   Individual employees, and not just the "covered entities" for whom they work, may be subject to HIPAA sanctions. Individuals found guilty of accessing PHI for personal gain have been subject to fines and jail time
6. **Disposal**
   - **a.** PHI must be disposed of properly
     - i. Paper PHI must be shredded or otherwise rendered illegible
     - ii. It is not sufficient to delete files containing electronic PHI. Media must be wiped clean and made irretrievable. This includes hard drives, flash drives, smart phones and other electronic devices, as well as some printers and copy/fax machines. Speak to your



2623 Hooper Avenue, Brick, NJ 08723 | Phone (718) 408-8989 | Fax (718) 650-6044 | Info@ComplianceCG.com | www.ComplianceCG.com

facility's Compliance Officer or HIPAA Security Officer for more information.

7. **Common Risk Areas / Standards of Reasonable Care / Policies & Procedures Required**
   - **a.** Paper records:
     - i. Are referrals or other paperwork being left unsecured? Are binders with patient information left unattended? e.g., med carts, exposed counter at nurses' stations
   - **b.** Copiers:
     - i. Is unprotected PHI being left at copy machines?
     - ii. is the copier hard drive erased properly before disposal or return to the leasing company?
   - **c.** Faxes:
     - i. Should be situated in protected area
     - ii. Are authorization instructions confirmed?
     - iii. Are fax numbers verified before sending? When possible, use pre-programmed numbers.
     - iv. Confidentiality statements should be included on all PHI communications.
   - **d.** Electronic PHI:
     - i. Are devices and emails properly guarded and encrypted?
     - ii. Is electronic PHI protected by individually assigned passwords and are log-in histories kept? Is there a BAA for technicians maintaining e-devices?
     - iii. Is PHI being saved on USB or other portable devices? Is there an inventory of all devices?
     - iv. Are employees trained to be aware of phishing scams?
     - v. Are screen savers automatically in place when a computer is unused?
     - vi. Is a process in place which requires lost devices to be reported immediately?
   - **e.** Phone calls / Texts:
     - i. Phone conversations should not be loud enough for non-authorized bystanders to hear.
     - ii. Transmitting text messages related to patient information (to either other employees/providers or family members) from any cellular device is highly discouraged. If absolutely needed, the message should be limited to minimum information necessary e.g. appointment confirmations, instructions to call the office to receive test results, etc.
   - **f.** Audio-Visual Recordings
     - i. Are allowed only in limited circumstances.
8. **Breaches**
   - **a.** An impermissible access, use or disclosure is generally considered to be a breach when the security or privacy of the PHI is improperly exposed, unless the covered entity can demonstrate, through an extensive risk assessment, that there is a low probability that the PHI has been compromised. These risk assessments will generally include the following factors (a) the nature and extent of the PHI involved (b) the person who used or received the PHI (c) whether the PHI was actually acquired or viewed (d) the extent to which the risk to the PHI has been mitigated (e) the date of discovery (f) a brief description of what happened (g) how the incident was discovered (h) a description or listing of types of PHI included in the incident (i) a description or summary of who received the PHI and what the recipient did with the PHI, if applicable (j) any other relevant information.
   - **b.** Response to the breach may include:
     - i. Mandated notifications without unreasonable delay to government agencies, individuals affected, and the news media.
     - ii. Statutory and regulatory Civil penalties:
       1. $50,000 per incident up to $1.5 million per incident for violations that are not corrected, per calendar year.
     - iii. Statutory Criminal Penalties:
       1. $50,000 to $250,000 in fines and up to 10 years in prison.
   - **c.** An employee who becomes aware of a potential breach must report it to the Compliance Officer or HIPAA Privacy Officer immediately. A thorough incident report must be completed. Potential breaches must be investigated and, if applicable, reported within a specific time frame. Missing the deadline for investigating and reporting is in and of itself a violation of HIPAA and may incur fines.
9. **Risk Analysis and Risk Management.**
   - **a.** Prevention is the best cure. The law requires a periodic risk analysis be performed to prevent potential breaches. The analysis is designed to ensure that standards of reasonable care are practiced in every area, including Administrative, Physical, and Technical. A proper analysis is designed to identify security risks, vulnerabilities, and threats. It will generally include the following steps:
     - i. Identifying the Scope of the Analysis
     - ii. Gathering Data
     - iii. Identifying and Documenting Potential Risks, Vulnerabilities, and Threats
     - iv. Assessing Current Security Measures
     - v. Determining the Likelihood of Threat Occurrence
     - vi. Determining the Potential Impact of Threat Occurrence
     - vii. Determining the Level of Risk
     - viii. Identifying Reasonable Security Measures and Documenting/Implementing a Comprehensive Security Plan
   - **b.** To decrease the likelihood of penalties and/or sanctions, facilities should demonstrate the review and implementation of proper safeguards, reasonable care, and appropriate compliance trainings.
   - **c.** The facility must also conduct an additional analysis upon the occurrence of a significant event or change in the Facility's organization or environment.
10. **Additional Topics**
    - **a.** Rules apply to *anyone* performing services, who by virtue of their position are likely to obtain access to PHI. i.e. employees, volunteers, trainees, and others under direct control of persons working on behalf of covered entity, even if not a contractor or business partner.
    - **b.** Privacy
      - General confidentiality
      - Training requirements
      - Resident rights (general)
      - Reporting known or suspected breaches
      - Sanctions
      - E-mail
      - Faxing
      - Complaints
      - Use of social media
      - Reporting potential privacy or security violations
    - **c.** Security Topics
      - General security policies
      - Physical and workstation security
      - Periodic security reminders
      - Virus protection
      - Importance of monitoring log-ins
      - Password management / log-in monitoring
      - Audits
      - Overlooking *minor* details can lead to *major* problems

***Please refer to the facility's Privacy and Data Security Policies and Procedures for further information.***



2623 Hooper Avenue, Brick, NJ 08723 | Phone (718) 408-8989 | Fax (718) 650-6044 | Info@ComplianceCG.com | www.ComplianceCG.com

*I understand and acknowledge that the Facility is committed to meeting all federal and state privacy and data security laws, rules, and regulations, including, but not limited to, HIPAA. I hereby acknowledge that I have received HIPAA privacy and security training, including a review of Policies and Procedures related to the handling, security, and confidentiality of resident/patient information, and have been afforded the opportunity to ask questions or seek clarification and all of my questions have been answered.*

*I understand that my obligations, as set forth above, will continue throughout my employment with the Facility and even after the termination of my employment. I understand that, to the extent that I violate my obligations hereunder or under any state or federal law, regulation or rule, I will be subject to disciplinary action, which may include termination, and I may also be subject to civil and criminal penalties under state and federal laws, regulations, or rules. By signing this form, I acknowledge that I understand the foregoing and will abide by the Facility's HIPAA Policies and Procedures.*

_____ _____

PRINT NAME TITLE/DEPARTMENT

_____ _____

SIGNATURE DATE

***Thank you for your partnership in keeping our residents' protected health information confidential and secure, and for recognizing its importance in facilitating quality health care!***



2623 Hooper Avenue, Brick, NJ 08723 | Phone (718) 408-8989 | Fax (718) 650-6044 | Info@ComplianceCG.com | www.ComplianceCG.com