COMPLIANCE CONSULTING GROUP, LLC

HIPAA Training and Education

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

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.

HIPAA Training and Education

I understand and acknowledge that the Facility is committed to meeting all federal and state privacy and date security rules and regulations, including, but not limited to, HIPAA. By signing this form, I acknowledge that I understand my ongoing responsibilities regarding the privacy of protected health information and will abide by the Facility's HIPAA Code of Conduct.

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.

_____ _____

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!

COMPLIANCE CONSULTING GROUP, LLC

COMPLIANCE COMMITTEE/ DEPARTMENT HEAD TRAINING
HIPAA PRIVACY

FACILITY NAME: _____

PRESENTED BY: _____ ON _____

1. Reviewed required elements of a Compliance Program
2. Provided an overview of HIPAA regulations
3. Provided an explanation of what information is considered to be PHI and the mediums that can be considered PHI (e.g. verbal, written, or electronic e-PHI)
4. An explanation of allowable uses and disclosures of PHI, for Treatment, Payment, or Healthcare Operations.
5. Some examples of incidental uses of PHI which are allowed
6. Restrictions and unallowable uses of PHI, including the minimum necessary restriction
7. Disposal guidelines for PHI, including e-PHI
8. Breach reporting and what do if a breach is suspected.
9. Common risk areas, including unlocked computers, papers or binders left unattended, unencrypted emails, portable devices
10. Other areas discussed include
    - Texting guidelines
    - Phishing scams
    - Social media guidelines
    - Restrictions on audio/visual recordings
11. Due to the large amounts of PHI and e-PHI used in the facility, it is inevitable to have instances in which there is a concern about a breach or impermissible use of PHI or e-PHI. Supervisors should encourage their staff to report problems and concerns so they could be properly addressed. Questions should be addressed to supervisors, the Compliance Officer, or the HIPAA Privacy and/or Security Officers. The anonymous Compliance Hotline may be used.

	Name	Signature	Title	Shift		Name	Signature	Title	Shift
1					15				
2					16				
3					17				
4					18				
5					19				
6					20				
7					21				
8					22				
9					23				
10					24				
11					25				
12					26				
13					27				
14					28				

Please send in completed Sign-in Sheet to trainings@compliancecg.com

COMPLIANCE CONSULTING GROUP, LLC

STAFF TRAINING
HIPAA PRIVACY

FACILITY NAME: _____

PRESENTED BY: _____ **ON** _____

1. Reviewed required elements of a Compliance Program
2. Provided an overview of HIPAA regulations
3. Provided an explanation of what information is considered to be PHI and the mediums that can be considered PHI (e.g. verbal, written, or electronic e-PHI)
4. An explanation of allowable uses and disclosures of PHI, for Treatment, Payment, or Healthcare Operations
5. Some examples of incidental uses of PHI which are allowed
6. Restrictions and unallowable uses of PHI, including the minimum necessary restriction
7. Disposal guidelines for PHI, including e-PHI
8. Breach reporting and what do if a breach is suspected
9. Common risk areas, including unlocked computers, papers or binders left unattended, unencrypted emails
10. Other areas discussed include
    - Texting guidelines
    - Phishing scams
    - Social media guidelines
    - Restrictions on audio/visual recordings
11. Questions should be addressed to supervisors, the Compliance Officer, or the HIPAA Privacy and/or Security Officers. The anonymous Compliance Hotline may be used.

	Name	Signature	Title	Shift		Name	Signature	Title	Shift
1					16				
2					17				
3					18				
4					19				
5					20				
6					21				
7					22				
8					23				
9					24				
10					25				
11					26				
12					27				
13					28				
14					29				
15					30				

Please send in completed Sign-In Sheet to trainings@compliancecg.com