COMPLIANCE CONSULTING GROUP, LLC

HIPAA INCIDENT CHECKLIST

In the event of an incident which may have involved an impermissible access, use, or disclosure of Protected Health Information ("PHI"), a HIPAA breach may have occurred. In such cases, the facility is required to investigate the incident and determine what steps must be taken.

This checklist is designed to guide your facility through the process of documenting, investigating, and addressing the incident. Please make sure to review every step in this checklist.

ITEM		COMMENTS AND ADDITIONAL INFORMATION
1	Assign responsibility for the overall investigation of this incident	• Generally, investigations related to Protected Health Information (PHI) are the responsibility of the HIPAA Privacy and/or Security Officers. The HIPAA Officer can choose to designate all or parts of the investigation to other individuals.
2	Include the incident in the appropriate logs.	• If the incident involves a family grievance, the Grievance Officer should be notified and the incident should be included in the Grievance Log. • The facility's Compliance Officer should include this incident in the Compliance Log.
3	Determine the date of the discovery	• Determining an accurate date of discovery is important because if the incident is determined to be a breach, the deadline for breach notification is dependent on the date of discovery. • The date of discovery should be documented on Attachment A: HIPAA Incident Documentation.

4	Assign an incident number	• To assist in tracking any outstanding responsibilities or results from the investigation, it is helpful to assign an incident number that can be used on all documents related to the incident. • A combination of year/month/incident is often used. For example, the first incident in March of 2007 could be Incident 07-03-1.
5	Collect basic information regarding the incident	• Use Attachment A: HIPAA Incident Documentation to document basic information related to the incident.
6	Investigate the incident	• The investigation should be detailed and thorough. • All steps taken in the investigation, including interviews, email correspondence, and other items should be documented and dated.
7	Conduct a Risk Assessment	• This assessment is required in response to an incident which may be a breach. • This process can be documented in Attachment B: HIPAA Risk Assessment, Analysis and Breach Determination.
8	Conduct a Risk Analysis	• An analysis of the Risk Assessment's factors is used to determine if the incident should be considered a breach. • This process can be documented in Attachment B: HIPAA Risk Assessment, Analysis and Breach Determination.
9	Determine if a breach has occurred	• This determination can be documented in Attachment B: HIPAA Risk Assessment, Analysis and Breach Determination.

10	Breach notification to the affected individuals	• If the incident is determined or presumed to be a breach, notification to the affected individuals is required. • Use Attachment C: Response to Presumed Breach to document appropriate or required actions.
11	Breach notification to the Secretary	• If the incident is determined or presumed to be a breach, notification to the HHS or OCR is required. • See Attachment C: Response to Presumed Breach for more information.
12	Breach notification to the media	• If the incident is determined or presumed to be a breach, notification to the media may be required. • See Attachment C: Response to Presumed Breach for more information.
13	Develop and Implement Corrective Action Plans	• If the incident is determined or presumed to be a breach, Corrective Action may be required. • If the incident is NOT determined or presumed to be a breach, Corrective Action may be advisable and appropriate. • See Attachment D: Corrective Action Plans and Follow Up for more information and to document applicable Corrective Action Plans and results.
14	Notify relevant internal or external individuals	• Administrators, supervisors of those involved, legal counsel and other relevant individuals should be notified, as appropriate. • If the incident involves a family grievance, the Grievance Officer should be notified. Response to a grievance may be required within a specific time frame.

15	Enforce any relevant disciplinary actions	• Enforcing disciplinary action is an important element of a compliance program.
16	Follow up on Corrective Action Plans	• Follow up in the form of audits, training, or other actions may be appropriate. • Use Attachment D: Corrective Action Plans and Follow Up to document and track applicable Corrective Action Plans.

ATTACHMENT A
HIPAA INCIDENT DOCUMENTATION

Assessment Information:

Facility Name: _____

Facility Address: _____

Incident number[1]: _____

Individual completing this form (name and title): _____

Date of discovery: _____

The date of discovery is the date on which the breach or incident is known to the facility, or, by exercising reasonable diligence, would have been known to the facility.

Number of affected individuals (estimated): _____

Summary of Incident:

The summary must include the following information:

- Date and time of incident
- Date, time and method the incident was discovered
- Date, time and method the incident was reported
- Location of incident (department/floor)
- Source or type of PHI (e.g. EHR, paper records, etc.)
- Number of individuals affected by the incident

[1] The incident number should be consistent throughout all documents regarding this incident.

ATTACHMENT B
HIPAA RISK ASSESSMENT, ANALYSIS, AND BREACH DETERMINATION

Assessment Information:

Facility Name: _____

Incident number: _____

Individual completing this form (name and title): _____

Date: _____

Risk Assessment- This risk assessment will be used to determine the likelihood PHI has been compromised. Each of the following four factors must be assessed.

Factor 1: Nature and Extent of PHI involved

In this space, include information such as what type(s) of PHI was involved; if the PHI was demographic, financial or clinical in nature; if the PHI contained sensitive information; if the PHI was de-identified or hard-to-identify, etc. For example, the PHI on a misplaced waiting room sign-in sheet contains PHI which is less sensitive than the PHI included in a misplaced folder with the patient's extensive clinical history. Similarly, the list of room numbers where salt-free meals should be delivered may contribute to a lower likelihood of compromise than a situation in which a resident's prescription is faxed to the wrong party.

Factor 2: Persons or Entity/Entities to which the PHI was divulged

In this space, include information as to who received the PHI; whether the recipient is a covered entity; if the recipient would be able to identify the information he/she received; or other factors that should be considered relating to the recipient of the PHI and how that will affect the likelihood the PHI was compromised.

Factor 3: Whether the PHI was actually acquired or viewed

In this space, include information on how the PHI was sent; whether or not it was received; or other related factors which will affect the likelihood the PHI was compromised. For example, a sealed envelope given to the wrong individual, which was returned unopened, will have a lower likelihood of compromise than an envelope that had been opened.

Factor 4: The extent to which the risk to the PHI has been mitigated

In this space, detail your facility's mitigation efforts to limit the access or exposure to the PHI involved and how those steps may affect the likelihood the PHI has been compromised or may further be compromised. Consider items like assurances that the information will not be further used or disclosed (e.g. through a confidentiality agreement) and whether or not the PHI has been (or is able to be) destroyed. Include information on the extent and efficacy of the mitigation.

Factor 5: Additional factors to consider (optional)

In this space, include additional factors which are relevant in determining the probability the PHI was compromised. If none, put N/A.

Risk Analysis

In this space, include an analysis of the factors listed in the assessment above. The analysis must result in a determination as to the level of likelihood that the PHI was compromised.

Breach Determination

By selecting one of the following choices, you will document a conclusion as to whether or not the incident under investigation is considered a breach, as per HIPAA guidelines.

Choose one of the following:

○ This incident was an unintentional acquisition, access, or use of PHI by an individual acting under authority of the covered entity which was made in good faith and within the scope of authority and did not result in further impermissible use or disclosure. As per HIPAA 45 CFR § 164.402(1)(i), this incident is NOT considered to be a breach. (Please refer to Attachment D for implementation of corrective action, if applicable.)

○ This incident was an inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same facility or business associate, and the PHI received as a result of this disclosure was not further used or disclosed in an impermissible manner. As per HIPAA 45 CFR § 164.402(1)(ii), this incident is NOT considered to be a breach. (Please refer to Attachment D for implementation of corrective action, if applicable.)

○ This incident involved an acquisition, access, use, or disclosure of PHI that analysis has shown to have a low probability that the PHI has been compromised. As per HIPAA 45 CFR § 164.402(2), this incident is NOT presumed to be a breach. (Please refer to Attachment D for implementation of corrective action, if applicable.)

○ This incident involved an acquisition, access, use, or disclosure of PHI that does not fall into any exceptions and which analysis did not demonstrate as having a low probability that the PHI has been compromised. This incident is therefore presumed to be a breach. (Attachment C **must** be completed.)

COMPLIANCE CONSULTING GROUP, LLC

ATTACHMENT C

RESPONSE TO PRESUMED BREACH

Assessment Information:

Facility Name: _____

Incident number: _____

Conducted by: _____

Date of discovery: _____

The date of discovery is the date on which the breach or incident is known to the facility, or, by exercising reasonable diligence, would have been known to the facility.

Number of affected individuals: _____

Breach Determination

Based on the assessment and risk analysis conducted by the facility (see Attachment B), this incident involved an acquisition, access, use, or disclosure of PHI that does not fall into any legally allowed exceptions and which analysis did not demonstrate as having a low probability that the PHI has been compromised. This incident is therefore presumed to be a breach.

Breach Notification to the affected individuals

Due to the fact this incident is presumed to be a breach, notification to the affected individual(s) is required. Notification must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The attached template may be used for breach notifications.

The written notice must include the following elements:

A description of what happened
A description of the types of PHI involved
Steps the affected individuals should take to protect themselves from potential harm resulting from the breach.
A brief description of what the facility is doing to investigate the breach, mitigate harm caused by the breach, and to protect against further breaches
Contact procedures for individuals to ask questions or receive additional information. This must include a toll-free telephone number, an email address, web site or postal address.

Notification Information:

In this space include information on how and when the notification was provided.

Breach Notification to the Secretary

Any breach of unsecured PHI requires notification to the Secretary. If the breach involved more than 500 individuals, notification must be submitted contemporaneously with the notice to the affected individuals. If the breach involved fewer than 500 individuals, a log should be kept and the information submitted to the Secretary not later than 60 days after the end of each calendar year.

Choose one:

- Notification to the Secretary must be submitted within 60 days of the date of discovery because the breach involved PHI of more than 500 individuals.
  Date of submission:
- Notification to the Secretary must be submitted within 60 days after the end of the calendar year because the breach involved PHI of fewer than 500 individuals.
  Date of submission:

Breach Notification to the Media

If the incident involved the PHI of more than 500 residents of a state or jurisdiction, notification to the media is required. Notification must be made without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

Choose one:

- Notification to the media was not necessary because the incident involved PHI of fewer than 500 individuals.
- Notification to the media is necessary because the incident involved PHI of more than 500 individuals.

The following media outlets were notified. _____

Date of notification _____

Additional information

Breach Mitigation The following steps have been taken to mitigate the breach.
Corrective Action Plan This breach has highlighted (one or several) weakness(es) in the facility's protection of PHI. In response, Corrective Action Plans have been established. Please refer to Attachment D.

ATTACHMENT D
CORRECTIVE ACTION PLANS AND FOLLOW UP

Incident Information:

Facility Name: _____

Incident number: _____

Responsible party (name and title): _____

Corrective Action Plan

This incident has identified areas in need of corrective action regarding the facility's protection of PHI. In response, the following Corrective Action Plans have been established.

Issue	Corrective Action	Responsible Party	Date of expected implementation	Status