Risk Assessment Guidelines for Breach of Data

(effective September 23, 2013)

Overview: The HIPAA Final Rule presumes a breach has occurred for every impermissible use or disclosure unless there is a low probability that the PHI was compromised. Your risk assessment must show analysis and documentation of how you reached your conclusion of low or high probability of compromise.

This Risk Assessment will help to determine the probability that the PHI was compromised.

1. **Identity the PHI and determined what happened.**
    a. Was it internal misuse or external disclosure?

    b. Was the PHI accessed, acquired, used, or disclosed in a manner not permitted by HIPAA?

    c. Was the PHI encrypted?

    <u>If PHI was encrypted, then a data breach has not occurred, and no further risk assessment is needed, but documentation must occur. No need to progress to #2.</u>

2. **Assess if any of the following HIPAA exceptions apply.**
    a. The access or use/disclosure was **unintentional,** made by a staff member in good faith, and within scope of job responsibilities

    b. The disclosure was inadvertent, made by an authorized person to someone also authorized to have access to PHI within covered entity or business associate, and, there is **no further use** or disclosure of the PHI

    c. The covered entity or business associate believes in good faith that the information disclosed in error **could not be retained** by the person receiving the information.

    <u>If any of the exceptions apply, document the exception and how it applies. There is no need to progress to Step 3.</u>

3. **If breach has occurred, and no exceptions apply, conduct a risk assessment, and document, at a minimum, the following factors:**

    1. What is the nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification? For example, how much PHI, how many patients, is there sensitive information such as Social Security or financial numbers?

    2. Who is the unauthorized person who used the PHI or to whom was the disclosure made? For example, was it a workforce member or someone not covered by HIPAA?

    3. Was the PHI actually acquired or viewed? For example, how much access was performed?

    4. To what extent has the risk to the PHI been mitigated? For example, what actions were taken to mitigate the harm to the patients?

Even if the breach is suspected, covered entities and business associates must exercise reasonable diligence in investigating the suspected breach.

The entity that holds the PHI has the **burden of proving** that a breach has not occurred.

Documentation must support if there is **a low probability** or a higher probability that the PHI was compromised**.** The following questions will help to determine probability.

What Information was Accessed, Used, or Disclosed?
Some information may offer more opportunities for misuse than others.

- Social Security Number: of significant concern because of the potential for identity theft
- Other ID numbers including account number, medical record number, etc.
- Demographics: date of birth is also a key piece of information for identity theft
- Diagnosis, Medical: some diagnoses are particularly sensitive (HIV/AIDS, cancer, cosmetic surgery)
- Diagnosis, Behavioral: these diagnoses are significant because of their sensitivity, as well as the fact that patients with these diagnoses may react especially strongly to notification
- Procedures: some procedures indicate particularly sensitive diagnoses
- Clinical Notes: provides details about health status, diagnosis, treatments
- Billing Information: may include procedural detail; high charges may indicate severity of illness

Who is the Recipient of the Patient's Information?

Lower Risk

- Another covered entity (Information in the hands of covered entities e.g. lab, hospital or doctor's office, would generally be less of a concern since they are regulated by HIPAA)
- A co-worker with no personal ties to patient
- A related family member involved in care. (Information disclosed to family member involved in the care of the patient would generally be less of a concern.)
- Based on your discussion with an external person or organization that has received the information, how likely do you think it is that they will misuse it? Are they willing to return the information?

Higher Risk

- An estranged family member
- Unrelated individual
- Employer: information disclosed to an employer could be used to make employment decisions
- Person or organization believed likely to misuse the information
- Internet
- Life insurance company or similar insurer that is not a covered entity
- Unknown: In a situation where the whereabouts of the PHI, or the identity of the person(s) who has the PHI is unknown, there is greater concern than if you know who has the PHI and you judge that the risk of misuse is low

Documentation must support whether or not **notifications are required**, and if so, that they were made in accordance with **HIPAA notification requirements.** For example, you must document that HHS will be or has been notified on an annual basis of this breach that affected less than 500 individuals. OR you must document that HHS was notified within 60 days of discovery of a breach that affected 500+ individuals.

Covered Entities may exercise their right to provide notifications to patients even if not required by HIPAA, i.e. even if low probability of compromise, OR in lieu of conducting a formal risk assessment.

Formally document every step of the process and retain it for at least six years from date of discovery**.**