Breach Risk Assessment Framework

Principles of the Framework

- Each individual breach case is unique
- Each investigation should follow the same process and criteria
- Analysis should guide a decision, but not the decision itself
- Provide consistent application, formal decision-making process with metrics, a methodology that can be documented and sufficiently flexible to modify for both state and federal breach definitions.

Some Considerations for Analysis of "low probability of compromise"- also see *Preamble to Omnibus Rule*

1. The nature and extent of the Protected Health Information (PHI) involved
    - What identifiers were involved?
    - What was the level of detail disclosed?
    - What is the likelihood of re-identification
    - What information was involved?
    - How can it be used?
    - How much PHI was involved?
    - Is the PHI old or current?
    - What is the likelihood that the information could be misused?
    - Is the content typically considered "sensitive"?

2. The unauthorized person who used the PHI or to whom the disclosure was made

- What was their reaction to receiving the information?
- Were they an unintended recipient or did they seek out the information?
- Following discovery, did they initiate contact with the affected individual(s)?
- Is there a relationship to the affected individual(s)?
- Is there a willingness to return the PHI?
- Was the recipient another covered entity or business associate?
- In the case of a family member being the recipient, is it likely that the recipient is already aware of the information?

3. Whether the PHI was actually acquired or viewed

- Was the access or disclosure a mistake?
- Was the access or disclosure intentional?
- Was the access or disclosure intentional for self-serving, malicious or harmful reasons?

4. The extent to which the risk to the PHI has been mitigated

- Was the information not further used or disclosed?
- Was the information immediately destroyed?
- Was the information immediately returned?

5. Retain documentation

- Document process and logic behind decisions, in case the breach notification decision is questioned.
- Ensure the process is:
    - Formal
    - Consistent
    - Measurable
    - Structured
    - Backed by evidence
    - Transparent
    - Objective
- Maintain incident logs, mitigation activity, corrective action plans, etc.