Breach Documentation Checklist

Items to capture in documentation of a privacy or security breach:

- □ Complainant name, and relationship to patient; contact information for both
- □ What PHI was compromised, how much PHI, and was any sensitive in nature?
- □ How many people are affected by the breach? If more than 500 you must contact HHS within 60 days of breach. You must notify HHS annually of all breaches less than 500.
- □ Date of incident and date of discovery. Date of breach notification to patient.
- □ Where did it happen, and how did the breach happen?
- □ What is the desired outcome by patient?

Completely document the follow up and your risk assessment:

- □ Whether the acquisition, access, use, or disclosure of the PHI violates the HIPAA Privacy Rule
- □ Whether the PHI involved was "unsecured" (usable, unreadable, or indecipherable/ encrypted)
- □ Whether an exception to the definition of breach may apply
- □ Whether there was a low probability that the PHI has been compromised

A risk assessment to determine whether there is a low probability that the PHI has been compromised must include consideration of the following four factors:

- □ The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- □ The unauthorized person who used the PHI or to whom the disclosure was made
- □ Whether the PHI was actually acquired or viewed
- □ The extent to which the risk to the PHI has been mitigated

Document why and how you, and others you consult with (Privacy Officer, Security Officer, etc.), arrived at the conclusion to which you came. Show your logic, thoroughness, conclusion, and thinking process.

Note: If Munson's Information Systems was breached, you may need to work with Linda Bower, Munson Security Officer, for a forensic analysis.

What is your resolution? What remedial action steps have been taken to prevent reoccurrence?

Examples:

- Offering credit monitoring to the affected individuals in the event that Social Security number or financial account data are involved in the breach
- Setting up a call center to address questions of affected individuals regarding the breach
- Improving existing policies or procedures
- Additional training of workforce members on how to safeguard PHI
- Encrypting portable media that contains PHI
- Requiring employees to change their passwords
- Increasing physical security through the use of biometric locks or other devices
- Sanctions to employee who violated breach policy, ranging from re-education to written warning to termination
- And in particular, identifying any gaps in compliance that led to the breach and closing those gaps to ensure that another similar breach will not occur
- When was the Breach Notification or other letter of communication sent to patient? What steps if any, are being taken to help protect patient from ID theft?