HIPAA/HITECH Decision Tree to Determine Whether Breach Notification is Required

**STEP 1:** Determine whether use or disclosure was permitted under Privacy Rule

- **YES:** NO BREACH NOTIFICATION REQUIRED
- **NO:**
  - **STEP 2:** Determine if PHI was unsecured or “limited”
  - **YES:** PHI was not secured by encryption or destruction
    - **NO:** Was the PHI limited to just a limited data set (no direct identifiers) and contain no dates of birth or zip codes?
      - **YES:** NO BREACH NOTIFICATION REQUIRED
      - **NO:**
        - **STEP 3:** Determine if an exception applies
          - **YES:**
            - **STEP 4:** Conducting risk assessment: Did use/disclosure pose a significant risk of financial, reputational or other harm?
              - **YES:** BREACH NOTIFICATION IS REQUIRED
              - **NO:** NO BREACH NOTIFICATION REQUIRED
          - **NO:**
            - **#1:** Was PHI was unintentionally accessed by a workforce member performing his/her duties?
              - **YES:**
                - **#2:** Was PHI inadvertently disclosed from one workforce member to another?
                  - **YES:**
                    - **#3:** Was PHI was disclosed to a person who reasonably would not have been able to retain that information?
                      - **YES:** BREACH NOTIFICATION IS REQUIRED
                      - **NO:** NO BREACH NOTIFICATION REQUIRED
                    - **NO:**
                      - **NO:** NO BREACH NOTIFICATION REQUIRED
                - **NO:**
                  - **NO:** NO BREACH NOTIFICATION REQUIRED
              - **NO:**
                - **NO:** NO BREACH NOTIFICATION REQUIRED
            - **NO:**
              - **NO:** NO BREACH NOTIFICATION REQUIRED
          - **NO:**
            - **NO:** NO BREACH NOTIFICATION REQUIRED
        - **NO:**
          - **NO:** NO BREACH NOTIFICATION REQUIRED