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"

→ PHI was not secured by encryption or destruction

↓

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

PHI was secured by encryption or destruction

↓

NO BREACH NOTIFICATION REQUIRED

#1: Was PHI was *unintentionally* accessed by a workforce member performing his/her duties? → YES

NO ↓

#2: Was PHI *inadvertently* disclosed from one workforce member to another? → YES

NO ↓

#3: Was PHI was disclosed to a person who reasonably would *not have been able to retain* that information? → YES

NO ↓

STEP 4: Conducting risk assessment: Did use/disclosure pose a significant risk of financial, reputational or other harm?

NO → **NO BREACH NOTIFICATION REQUIRED**

YES ↓

BREACH NOTIFICATION IS REQUIRED