HIPAA Breach
Risk Assessment Analysis Tool

Note: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule

Q#	Question	Yes - Next Steps	No - Next Steps
	Unsecured PHI		
1	Was the impermissible use/disclosure unsecured PHI (e.g.. not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary)?	Continue to next question	Notifications not required. Document decision.
	Minimum Necessary		
2	Was more than the minimum necessary for the purpose accessed, used or disclosed?	Continue to next question	May determine low risk and not provide notifications. Document decision.
	Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?		
3	Was it received and/or used by another entity governed by the HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 & FISA of 2002?	May determine low risk and not provide notifications. Document decision.	Continue to next question
4	Were immediate steps taken to mitigate an impermissible use/disclosure (ex. Obtain the recipients' assurances the information will not be further used/disclosed or will be destroyed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
5	Was the PHI returned prior to being accessed for an improper purpose (e.g., A laptop is lost/stolen, then recovered & forensic analysis shows the PHI was not accessed, altered, transferred or otherwise compromised)?	May determine low risk and not provide notifications. Document decision. Note: don't delay notification based on a hope it will be recovered.	Continue to next question
	What type and amount of PHI was involved in the impermissible use or disclosure?		
6	Does it pose a significant risk of financial, reputational, or other harm?	Higher risk - should report	May determine low risk and not provide notifications. Document decision.
7	Did the improper use/disclosure only include the name and the fact services were received?	May determine low risk and not provide notifications. Document decision.	Continue to next question

8	Did the improper use/disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), ***or*** the information increases the risk of ID Theft (such as SS#, account#, mother's maiden name)?	High risk - should provide notifications	Continue to next question
9	Did the improper use/disclosure ***not*** include the 16 limited data set identifiers in 164.514(e)(2) ***nor*** the zip codes or dates of birth? Note: take into consideration the risk of re-identification (the higher the risk, the more likely notifications should be made).	High risk - should provide notifications	May determine low risk and not provide notifications. Document decision.
10	Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals (ex. Limited data set included zip codes that based on population features doesn't create a significant risk an individual can be identified)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
Specific Breach Definition Exclusions			
11	Was it an unintentional access/use/disclosure by a workforce member acting under the organization's authority, made in good faith, within his/her scope of authority (workforce member was acting on the organization's behalf at the time), and didn't result in further use/disclosure (ex. billing employee receives an e-mail containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected e-mail & deletes it)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
12	Was access unrelated to the workforce member's duties (ex. did a receptionist look through a patient's records to learn of their treatment)?	High risk - should provide notifications	Continue to next question
13	Was it an inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same organization, or its OHCA, ***and*** the information was not further used or disclosed (ex. A workforce member who has the authority to use/disclose PHI in that organization/OHCA discloses PHI to another individual in that same organization/OHCA and the PHI is not further used/disclosed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
14	Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (Ex. EOBs were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable)?	May determine low risk and not provide notifications. Document decision.	Continue to next question. Note: if the EOBs were not returned as undeliverable, these should be treated as breaches.

15	Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (ex. A nurse mistakenly hands a patient discharge papers belonging to a different patient, but quickly realized the mistake and recovers the PHI from the patient, and the nurse reasonable concludes the patient could not have read or otherwise retained the information)?	May determine low risk and not provide notifications. Document decision.	Document findings.
Burden of Proof: Required to document whether the impermissible use or disclosure compromises the security or privacy of the PHI (significant risk of financial, reputational, or other harm to the individual).			