Ss -- HIPAA Omnibus
Breach Analysis Form

Sections 1 & 2 -- HIPAA Violation and Breach Assessment		
Section 1: **Did an impermissible acquisition, access, use, or disclosure of PHI occur, including one or more of the following:**	**Yes / No**	**Comments**
1. Was the accessed, used or disclosed PHI more than the minimum necessary?		
2. Did the PHI include sufficient information to identify individual(s)?		
3. Was the impermissible accessed, used or disclosed PHI in an unsecured format?		
If the answer to any of these questions is 'Yes' you have a probable HIPAA privacy rule violation which is presumed to be a HIPAA breach unless proven otherwise. Proceed to the next section. ***If all are 'No' complete your mitigation and documentation, then close this incident.***		
Section 2: **Do any of the following Breach exceptions apply?**	**Yes / No**	**Comments**
1. Unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.		
2. Inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate.		
3. Does the covered entity or business associate have a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.		
If the answer to any of these questions is 'Yes' complete mitigation and your documentation, then close this incident. ***If all are 'No' proceed to Section 3 - The Low Probability of Compromise Analysis.***		

Section 3 -- Low Probability of Compromise Analysis		
The following questions are intended as a guide in determining if this HIPAA privacy rule violation, after thorough analysis results in a 'Low Probability of Compromise of the PHI' determination and is therefore not considered a HIPAA breach that requires notification. The following HIPAA 4 'factors' (in Bold) should be answered and weighted in a reasonable manner. This completed form will assist you in making the final breach determination for this incident based upon the evidence analyzed.	**Sensitivity of the PHI**	**Comments**
Rank the sensitivity of the disclosed PHI as one of the following: **HIGH** 'Super-confidential' type PHI based upon the inclusion of clinical elements or individual personal identifiers that may be subject to identiy theft. **MODERATE** Non 'super-confidential' PHI with a limited set of individual identifiers that are less vulnerable to identity theft. **LOW** PHI contains very limited data set and few, if any clinical or identity theft vulnerable data elements.		
Please answer the following questions related to the circumstances of this incident in regards to whether there was a low probability that the PHI was compromised by the impermissible access, use or disclosure.	**Low Probability? Yes/No**	**Justification**
1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;		
1a. Did the accessed, used or disclosed PHI contain direct patient identifiers?		
1b: Was the impermissibly accessed, used or disclosed PHI of a more sensitive nature?		
1c. Did the use or disclosure of PHI reveal a well-known person?		
1d. Does the amount of PHI accessed, used or disclosed increase the risk of compromise?		

	Low Probability? Yes/No	Justification
1e. Did the PHI include sufficient indirect patient identifiers that there is a likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other available information?		
2. The unauthorized person who used the protected health information or to whom the disclosure was made;		
2a. Does the unauthorized recipient have obligations to protect the privacy and security of the impermissibly accessed, used or disclosed PHI?		
2b: Does the recipient of the PHI have a relationship to the patient where they are likely to act in the patient's best interest?		
2c: Was the person who accessed, used or disclosed the PHI malicious in their intent?		
2d: Was the attitude of the recipient cooperative and supportive of the patient's confidentiality and privacy?		
2e: Was the recipient unintended or did they seek out the PHI?		
2f. Does the individual to whom the PHI was inappropriately accessed, used or disclosed have the ability to re-identify the individual(s).		
3**. Whether the protected health information was actually acquired or viewed; and**		
3a. Is it possible to demonstrate that the disclosed PHI was never, accessed, viewed, acquired, transferred or otherwise compromised?		
3b: Was the PHI returned intact and in a timely manner?		
4. The extent to which the risk to the protected health information has been mitigated.		
4a. Have you obtained the recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed?		

	Low Probability? Yes/No	Justification
4b: Do you have a good faith belief that the impermissible recipient will honor their assurances that they will not further use or disclose the PHI?		
4c. Has an effective mitigation strategy, policies and procedures been implemented that minimize the likelihood of re-occurrence of this type of impermissible access, use or disclosure of PHI?		
Final HIPAA breach determination: Based on the total of the evidence and answers above does this incident have a 'low probability of compromise of the PHI' based on HIPAA regulations?		
If your answer to the above line item is 'No', that there is not a low probability that the PHI was compromised this incident is then finally determined to be a HIPAA breach that requires notification to the individual(s) and the federal government.		
If any of the individuals whose personal or protected health information was potentially compromised by this incident were residents of a state that has also implemented breach regualtions be sure to integrate breach analysis specifc to that state into your determination and notification plans.		