Potential Breach Number:	
Date of Incident	
Date of Discovery:	
# of Patient Affected:	
PHI Involved:	

RISK FACTORS	EVALUATION QUESTIONS	FACTOR EVALUATION/ MITIGATION	LIKELIHOOD	IMPACT	SCORE(=LIKELIHOOD x IMPACT)
Nature and Extent of PHI Involved:	*The goal of evaluating this factor is to determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests.*				
	Which patient identifiers were used or disclosed? Does the combination of identifiers used or disclosed increase risk? Are there particular identifiers such as a SSN that raise concerns?	patient name, DOB, US report			0
	Does the PHI used or disclosed contain a senstive diagnosis? (e.g. substance abuse, mental health, STD, HIV, cancer)	no sensitive diagnosis disclosed			0
	Does the amount of PHI used or disclosed increase the risk?	small amount of PHI disclosed			0
	Does the use or disclosure reveal the PHI of a well-known individual?	no well-known individual			0
	Does the PHI used or disclosed include sufficient indirect patient identifiers that could make re-identification of individuals possible?	re-identification is moderate			0
Unauthorized Person to whom disclosure was made:	*The goal of evaluating this factor is to determine the probability as to whether the recipient might further use or disclose the PHI in a manner adverse to the individual or for the recipient's own interests.*				
	Does the unauthorized recipient have obligations to protect the privacy and security of the disclosed information such as a BA or another CE?	Yes because they are a CE			0
	Is the recipient a member of your internal workforce or a BA such that you can ensure that the PHI will not be further used or disclosed?	no			0
	Does the recipient have a relationship with the individual where they are likely to act in the individual's best interests?	no			0
	Is there additional risk if the recipient likely knows the subject of the PHI?	yes, but recipient provided satisfactory assurance that the PHI would not be used or disclosed			0
	If the recipient impermissibly used the PHI, what was their purpose or motive for doing so? --Unintentional or inadvertent error? --Intentional for self-serving, malicious, or harmful reasons?	no impermissable use or disclosure			0
	What was the attitude and demeanor of the unauthorized recipient? Was he/she cooperative and willing to work with you to secure the PHI? Was he/she concerned about protecting the PHI? Did he/she initiate contact right away, or did he/she appear reluctant to cooperate as leverage for something else he/she wanted for his/her own best interests?	She was cooperative and assured us she would destroy PHI. Satisfatory assurances that she would shred the PHI were given.			0
	Was the recipient an unintended recipient or did he/she seek out the information?	unintended recipient but infomation not sought			0
	If only indirect indentifiers were disclosed, does the recipient have the ability to re-identify the PHI?	most were direct identifiers			0
	Is it believed that the PHI was taken with intent to use or sell?	no			0
The acutal use of the PHI disclosed:	*The goal of evaluating this factor is to determine whether or not the PHI was actually acquired or viewed or whether there was an opportunity for the PHI to be acquired or viewed. The probability of comprimise is lower only if the opportunity existed for the PHI to be acquired or viewed but the PHI was not acutally acquired or viewed.*				
	Was the PHI actually acquired or viewed by an unauthorized person?	yes, but likelihood of re-disclosure is low			0
	It is possible to demonstrate that the PHI was never accessed, viewed, or acquired?	N/A			0
	If an electronic device is involved, does forensic analysis show that the PHI was accessed, acquired, viewed, transferred, or comprimised?	N/A			0
	If ePHI is involved, what does the audit trail indicate? What actions (e.g. print, view) were taken? What parts of the record were accessed?	N/A			0
The extent to which the risk to the PHI was mitigated:	*The goal in evaluating this factor is to determine how thoroughly and quicky the PHI involved has been secured following the impermissable use or disclosure.*				
	If the recipient was a CE or other reliable business otherwise bound by privacy obligations (e.g. BAs, banks or attorneys), was verbal confirmation given and documented that PHI was destroyed?	Yes			0

	If the recipient was not a CE or other reliable business otherwise bound by privacy obligations, was written confirmation of destruction obtained?	N/A			0
	If the recipient was an employee who impermissibly used PHI, was a statement of assurance obtained attesting the PHI will not be further used or disclosed?	N/A			0
	Has satisfactory assurance been obtained from the unauthorized recipient that the disclosed PHI will not be further used or disclosed or will be destroyed? Has an effective mitigation strategy been implemented such that further unauthorized disclosures are extremely unlikely?	Yes. Recipient at physician's office assured us that PHI was destroyed. Mitigation strategies were put into place.			0
	Was the PHI returned in a timely manner and intact?	PHI was destroyed			0
Overall Assessment	*Note: If any factor is scored great than 10 (Minimal or Low), the probability of comprimise is moderate to severe suggesting appropriate breach notification.*				
Comments					
Conclusion	Based on the factors noted above, there is a **LOW** probability that PHI has been comprimsed; therefore, NO breach reporting required under HIPAA.				
	Based on the factors noted above, there is a **HIGH** probability that PHI has been comprimsed; therefore, breach reporting required under HIPAA.				