

PRSN Breach Determination and Risk Assessment Tool

Description of the Incident

Date of Incident:		Date Reported to HIPAA Officer:
Date of Discovery:		
Name of person who discovered incident:		
Circumstances under which the discovery was made:		
Description of Incident:		
Specific data elements involved:		
Staff Person(s) involved:		
Number of individuals for whom a breach may have occurred:		
Names of individuals for whom their may have been a breach (if more than 10 attach list):		
Format of potential breach (i.e. fax, lost media device, e-mail, verbal, etc.):		
Other Information:		

Situations Excluded from Breach Definition

If all of the following are true, the incident does NOT constitute a breach, and no further analysis is needed:			
If the recipient of the information was a workforce member or person acting under the authority of a covered entity or a business associate, and:			
	Question	Yes/No	Justification/Explanation
	The disclosure, acquisition, access, or use of protected health information was unintentional or inadvertent,		
	The acquisition, access, or use of protected health information was made in good faith and within the scope of authority		
	The disclosure, acquisition, access, or use did not result in any further use or disclosure in a manner not permitted by the Privacy rules described in Policy 5.07 of this manual		
	If the information was disclosed to an unauthorized person, was the recipient of the information unable to reasonably to retain the information?		

Potential Breach and Risk Analysis

Determine whether incident was a potential breach:			
	Question	Yes/No	Justification/Explanation
1	Was the information that was acquired, accessed, used, or disclosed unsecured protected health information?		
2	Was the acquisition, access, use, or disclosure in violation of the Privacy rules as described in Policy 5.07 of this manual?		
If yes to both questions, the incident was a potential breach.			
Determine whether the potential breach compromises the security or privacy of the protected health information:			
3	Did it include any of the following identifiers? (check the identifiers included in the breach)		
	Names		
	Date of Birth		
	Zip Code		
	Postal Address information (excluding town, city, or State)		
	Telephone numbers		
	Fax numbers		
	Electronic mail addresses		
	Social Security Number		
	Medical Record Number		
	Health plan beneficiary numbers		
	Account numbers		
	Certificate/license numbers		
	Vehicle identifiers or Serial numbers, including license plate numbers		
	Device identifiers and serial numbers		
	Web Universal Resource Locators (URLs)		

	Internet Protocol (IP)		
	Biometric identifiers, including finger and voice prints		
	Full face photographic images or any comparable images		
If any of the above identifiers were involved, determine whether risk of financial, reputational, or other harm is significant:			
4	Does the breach pose a significant risk of financial, reputational, or other harm to the individual?		
	Consider the following questions and describe answers to the applicable questions in the right hand column prior to final conclusion:		
	Is the recipient obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information?		
	Does the level of detail that was disclosed, accessed, or acquired provide enough information to pose a significant risk of harm to the individual? (i.e. was the information of a specific or sensitive nature?)		
	Does the information include information that increases the risk of identity theft (such as a social security number, account number, or mother's maiden name)?		
	How likely is it that an individual can be identified by the identifiers available in the disclosure (i.e. if zip code was the only identifier, what is the risk that the individual could be identified, and subsequent harm could come to that individual)?		
	Has the entity responsible for the breach obtained satisfactory assurances that the information will not be further used or disclosed (such as through a confidentiality agreement or similar means)?		
	Has the entity responsible for the breach taken any other actions to mitigate harm to the individual(s)		
	Describe other potential risks:		
Financial Harm Risks:			
	Potential Risk	Level of harm risk estimated:	Justification
Reputational Harm Risks:			
	Potential Risk	Level of harm risk estimated:	Justification
Other Harm Risks:			
	Potential Risk	Level of harm risk estimated:	Justification
If answers to 1-3 are yes, AND the above analysis reveals a risk of significant harm a breach notification must occur in accordance to the PRSN Breach Notification Policy 5.16			