Breach Risk Assessment

According to the new HIPAA Omnibus Rules, any "impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity demonstrates that there is a low probability that the…information has been compromised". So, breach notification is necessary in all situations unless a risk assessment demonstrates that there is a low probability that the protected health information has been compromised.

A risk assessment must consider the following four factors:

1. The nature and extent of the information involved, including the type of information (was it names only, or was it names and social security numbers);
2. Who was the disclosure made to, or who used the information improperly (was it an identity thief, or was the wrong info faxed to the wrong doctor);
3. Was the information actually accessed or viewed, or was only the potential for disclosure an issue;
4. The extent to which the risk has been mitigated.

Here are the basics. First, evaluate what type of information was potentially compromised and how much was actually disclosed. If you have a situation where only patients' names were disclosed, but no other information, that is much less of a problem than if the patients' social security numbers and dates of birth were disclosed.

Second, consider who received the information. For example, what if you had a situation in which you accidently faxed the wrong patient's information to a specialist; they then called and said that you sent this information to the wrong doctor but they destroyed it as soon as they realized the mistake. Because they are a doctor you are familiar with and they are also a health care provider who is under HIPAA constraints, it is unlikely the information would be used improperly. In this case, it is likely that a completed risk assessment would show little likelihood that the information was compromised, so no breach notification would be necessary. In that case, you would just finish the risk assessment, document your findings and place it in your HIPAA notebook to show you properly evaluated the situation. On the other hand, if you accidently faxed a patient's medical record to his employer, that's an entirely different situation and it is likely that notification would be necessary.

Next, determine whether the information was actually acquired or viewed or if there was only the potential. For example, if you had a laptop stolen and the cops caught the guy coming out the back door before he had a chance to do anything with it, it is unlikely that a risk assessment would show that to be a reportable breach. If an EOB was mailed to the wrong patient, and it was returned to you unopened, a risk assessment would show that the information had not been compromised; if the patient received it, opened it, and called you to tell you they got the wrong bill, that information had been compromised.

Finally, consider the extent to which the risk to the information has been mitigated. In some situations, it is possible to determine that there is little risk that the compromised information will be used improperly. For example, if the wrong type of patient information is sent to a business associate or employee and they assure you the information was immediately destroyed and will not be used, the likelihood that the information will be disclosed is minimal. Or, if the information is sent to an unauthorized person, and they sign a confidentiality agreement assuring that the information will not be used or disclosed, depending on the situation, that may be sufficient to prevent improper usage of the information.

A risk assessment must be done thoroughly, completely, in good faith, and the conclusions have to be reasonable. If it is determined that a breach has occurred, the notification process must begin. If it is determined that no breach has occurred, place the completed assessment in your HIPAA notebook.

Breach Risk Assessment

Date of Incident (or Notification Date):	**Number of individuals affected:**
Summary of Events:	
1. Type of Information (names/social security/credit card numbers/clinical information/medical history):	
2. Who received/used the information:	
3. Was the information actually acquired or viewed (explain):	
4. Has the risk been mitigated so that the entity is assured the information will not be used (and if so, how?):	
After completing the risk assessment, it has been determined: ___This is a breach requiring notification, and breach requirements will be followed ; OR____ This is not a breach and notification is not necessary	