

## WHAT YOU COULD EXPECT IF YOU HAVE A DATA BREACH

By Sheryl J. Cherico, CEO, Tier3MD

July, 2014



If you have a data breach, expect to get a letter from the Office of Civil Rights (OCR) asking for various documentation and information. At first, it can be intimidating, but if you have completed a security risk analysis, you most likely have the information available. If you have not, the following information is useful in knowing what you need in your office to make sure you have all your ducks in a row.

The first thing they are going to ask you for is an admission, denial, or a statement indicating that you have obtained insufficient evidence to make a determination regarding the allegations. After that, they will want to see documentation of your internal investigation. Be prepared to have a response that you could send them. Once you have all of that, you will need documentation of your corrective actions.

What did you do to “fix” the problem? A good example is:

Susie posted a picture of a baby on facebook and tagged it “cutest baby ever”. Your documentation would say: Susie was reprimanded by our HR department and has been given a written warning. We have re-trained her on HIPAA policies and procedures in our office. Facebook was blocked and a new policy for social media was created for our office.

You will then be asked to send a copy of any existing policy, and new policy. In addition, you will be asked to send evidence that facebook has been blocked and the employee was retrained. Look at it this way... you need to provide proof by way of documentation for every single thing you did for the breach.

Documentation, documentation, documentation. I can’t say it enough times. Of course the best practice would be to have all your documentation prior to a breach. Having that in order may even prevent the breach. You will be asked for your policies. I hope you have them!

Sheryl is a HIPAA consultant for Tier3MD and has extensive experience in HIPAA security and risk procedures.