## How Much More Can I Do?
## Do You Think You've Done Enough?

Forgetting the fact that HIPAA is law, not just suggested 'best practices', the Director of HHS Leon Rodriguez said during the 2013 National HIPAA Summit, 'one of the major reasons for all of these policies and procedures is to instill patient trust.' Nevermind there may be an audit or a breach, which would require additional time, staff and money to survive. Can you be absolutely certain the current procedures you have in place fully protect patient privacy?

Take off the table that HIPAA is a task (although it is), or takes too much time (although it may), or costs too much (although it can). As a business person managing a successful practice, is it worth the effort? I recently listened to a webinar, and this very good point was highlighted: Risk = Threat x Vulnerability x Consequence. FBI Special Agent Lizabeth Lehrkamp said, *"If you want to do anything for security, you have got to prove that there is a reason for it. And that reason better be money. Nobody wants to pay for security, because it doesn't make anybody money. But consider this. Threat - someone stealing your patient data. Vulnerability - an unencrypted laptop. The consequence? Where do you start? Are you going to get sued? Do you need to notify, which could mean you lose business and trust."* The consequences are never ending!

We've been doing this for more than a minute. If there's a reason not to look further into a compliance plan, we've heard it. Doing the minimum is not an option. Having a scripted plan won't cover it. Developing and nurturing a "culture of compliance" should be your goal. Avoid these typical pitfalls:

***I can do this on my own...***
The Office of Civil Rights (OCR) referenced 10% of those that were randomly audited in 2012 had no clue what was going on. Others knew, but didn't have the 'dedicated" time or resources needed to implement accurate and thorough policies and procedures. Have you? Not the templates, but effective policies. The Omnibus Final Rule contains 563 pages alone; let alone the base laws the preceded it. *We'd like to help!*

***I simply don't have the time...***
As it is, we KNOW there is not enough time to do all that is required of you each day. We also run out of daylight. One of the presenters at the 2013 National HIPAA Summit mentioned HIPAA has been in place since... uh, well… 1996. And even if you didn't jump right on the bandwagon, HITECH was introduced in 2009. The Omnibus Final Rule went into effect in March of 2013. Catch-up may be difficult. *We have options that can help!*

***I've already done a risk Analysis...***
Or have you? Referencing the 2012 random audits, HHS discovered that many who felt they had done a risk analysis were actually just provided checklists. There is a good deal more to the Security Risk Analysis recommended for HIPAA. Detailed analysis, documentation and research are required to complete the Risk Analysis process as intended by the Security Rule. And... having done a Security Risk Analysis without implementing a plan is another 'issue' noted by HHS. Our clients understand the differences, and have been assisted with 'effective' policy creation and implementation! *We have helped!*

***Then… There is the Doctor(s)***
The doctor(s) won't spend that kind of money. We UNDERSTAND how hard it is, or has been, to convince your doctors what it is you need to do. For trying, you should be commended. It's as difficult to

acknowledge to yourself that you might be missing something, but can't seem to find the funds to discover where the gaps may be. If the money is not there for proper training and analysis, will it possibly be there for an audit? Would you rather prepare for the worst, or fight against it and hope for the best? *We offer payment plans that can help!*

There may be a cost to properly understand, design and maintain a HIPAA plan. But it'd be far less than the potential consequence of dealing with a breach. Risk = Threat x Vulnerability x Consequence. Outside of a penalty that may be assessed, the time and money for discovery, legal fees, credit monitoring cost, additional time or staff needed to fix the problem are all just a few things that should be considered.

Special Agent Lehrkamp said the government considers Healthcare 'Critical Infrastructure'. The data that you possess can be considered as valuable as our weapons secrets. We need to take compliance off of your 'To Do' list, and get it into practice. The Kardon Compliance Coaching webinar series, K-Complete Staff training portal and a slew of Compliance Officer training products allows you to handle tasks a little at a time and slowly implement an environment that reflects HIPAA awareness; for the Compliance Officer, the staff and your wisely selected BA's.