Susan Zinder, Esq.
szinder@zinderlaw.com
646-380-6715

HIPAA/HITECH Compliance for Attorneys and IT Consultants that deal with Medical Institutions (Hospitals, Medical Practices, Medical Billers, Radiology, Pharmacies, etc)

So, your client (or your client's client) is a medical practice or other healthcare provider, and they've sent you this "Business Associate Agreement" ("BAA") to sign on top of your services agreement, and they want to know the ins and outs of how you secure their patient information; and you're thinking, "I don't need to do this."

Well…. THINK AGAIN!!!!

On March 26, 2013, long awaited federal regulations under the Health Insurance Portability and Accountability Act (popularly known as "HIPAA") were finally made public and quite possibly **THESE REGULATIONS APPLY TO YOU AND TO YOUR BUSINESS!**!!

If, as part of the services you provide to your clients **you receive, create, maintain, or transmit the individually identifiable health information of patients of your clients (or your client's client)**, then odds are high that you need to comply with the new HIPAA regulations. If you are a lawyer and your client has sent you information about their patients; if you are an IT provider and you maintain information about your customer's patients on your servers; these regulations apply to you. Lawyers, your ethical obligations to your clients will not get you out of complying with these regulations. IT providers, the storage of the information on your subcontractors' servers will not get you out of complying with these regulations.

Now what do you do? The following is a starting list, but depending on the information and your activities it may not be complete, so you should also consult with professionals experienced in this area.

- **Identify someo**ne in your organization, and charge them as your security officer with responsibility for your compliance.
- **Complete a Risk Assessment** of the potential risks created by your business processes:
    - **Understand**, for each of your clients, what information you are receiving, creating, maintaining how you are doing so.
        - Is the information only on a server?

        - Do you control the server or is its control subcontracted out?
        - Is it accessible through a PDA or other wireless device?
    - Understand to whom (and why) you may be transmitting that information. Are you delegating any of your contractual obligations, functions, activities or services to another entity? If so, how are they receiving, creating, maintaining or transmitting the individually identifiable health information you are sending to them. Just like you will have to provide this to your client, they will have to provide it to you.
    - **Assess** your current HIPAA compliance. Do you use and disclose the information only as permitted by law and within the terms of the BAAs you have signed?
        - When using or disclosing the information, are you only asking for, and accessing, the "minimum necessary"?
    - Have you implemented "**Administrative, Physical and Technical Safeguards**" intended and designed to respond to what you have learned in your risk assessment? For example:
        - Administrative safeguards include (but are not limited to) **written** policies and procedures that you have in place and on which you have trained your staff.
        - Physical safeguards include (but are not limited to) locks on the rooms where your computers and servers are stored, locks on each of the computers, devices and servers themselves.
        - Technical safeguards include (but are not limited to) effective passwords on the computer, device, and file, and potentially, encrypting the data.
        - **Remember, passwords and encryption are critical to protecting the information**.
- If you haven't yet, **IMPLEMENT** those safeguards as soon as possible:
    - Prepare contingency plans for disaster recovery, etc… if an event or disaster interferes with normal access to and processing of the information.
    - Speaking of Administrative Safeguards, make sure they address:
        - How to handle remote access and portable devices
        - Authorizations, passwords (don't share them), and workstation use
        - Risk management
        - Workforce security
        - What to do if there is a breach
        - Employment sanctions for when your policies aren't followed
- **TRAIN** your workforce (and if you have already done so, train them again)
- **COMMUNICATE** your policies and requirements to any subcontractors
- Review and **revise** (often with your attorney) your Business Associate Agreements.

- **DOCUMENT, DOCUMENT, DOCUMENT** everything that you are doing to comply and your plans for future compliance. Remember, it is the government's position that if you can't document what you have done, you haven't done it.
- **Consider cyber liability insurance.** This can, if written properly for limits you can afford, provide you with some financial protection if a breach occurs.

Great but if the data is still breached you have more work to do, including, potentially, reporting the breach to your client and possibly the government. But, what you do NOW to comply, the resulting safeguards you implement, and your response to any breach, will be what protects you from the otherwise significant fines and penalties that the government can impose.

SO, BE AWARE, ASSESS YOUR BUSINESS PROCESSES, TAKE ACTION TO MINIMIZE THE RISK, AND GET HELP TO MAKE SURE YOUR ACTIONS ARE COMPLETE, preferably from an IT security expert or an experienced healthcare lawyer.

Susan Zinder is a healthcare IT attorney, with over 20 years representing healthcare organizations from both the in-house and outside counsel perspectives. During her career, she has helped her clients successfully negotiate and implement clinical, ancillary and financial systems, including ambulatory care electronic medical records systems. She has also successfully implemented IT solutions for her own department's processes. Susan may be reached at szinder@zinderlaw.com