The Mental Health Professional's Workbook for HIPAA Security Compliance

Find full information at: https://www.personcenteredtech.com/goworkbook

The Workbook's Introduction and "Table of Contents"

Below you'll find the introduction to the workbook. It will provide a brief overview of all three books of the workbook and the kinds of activities you'll do in them.

This introduction is from the testing version of the workbook, and will likely go through many changes – including being turned into easy, interactive software.

Enjoy!

What Do I Do With This Thing?

This workbook is meant to help what we call "tiny" mental health practices perform the essential functions of compliance with the HIPAA Security Rule. Namely:

1. Perform and document an "accurate and thorough" Risk Analysis.
2. Document a Risk Management Plan based on the Risk Analysis.
3. Create a set of Policies and Plans that help you put your Risk Management Plan into action, and also helps you keep on top of certain security requirements that HIPAA has for us.

The workbook will take you through these processes step-by-step, chunked down into pieces to make it all manageable. The workbook also includes thorough worksheets and reference guides for examining each kind of resource you use in your practice, e.g. smart phones, computers, file cabinets, etc. And we provide you with a pre-created set of Security Policies you can adopt into your practice, along with specific instructions and templates to take you through the process of putting those Security Policies into effect.

All the worksheets and the pre-created Security Policies are designed to fit best with mental health practices that have between one and a few clinicians and perhaps a couple of other folks who help run the practice, which we call "Helpers" in this workbook.

So to get started, just keep reading. The workbook will guide you through what to do.

What Are the Things I'm Going to be Doing?

You'll be doing three things as you complete the workbook.

1) Risk Analysis *(AKA Book 1, coming around May 31st)*

Security Risk Analysis is a holistic process of examining all of your practice resources together as a **system**, looking for the ways they interact with each other and for security problems that need to be addressed.

Risk Analysis is not unlike doing a genogram with clients. It's a thorough, systems-minded way of understanding the whole picture of the information-related resources you use in your practice. As we well know in our work, understanding the whole picture is the first real step to positive and effective change.

Risk Analysis is known by research to be the strongest way to start an ongoing process of making sure your clients' sensitive and confidential information is protected from getting into the wrong hands. It also helps you keep your practice running without losing important information that you need to keep practicing.

It's also required by the HIPAA Security Rule, of course.

Your Risk Analysis will start with a process of brainstorming and identifying the "family tree" of resources in your practice that "touch" important information. You'll see which companies are part of your practice's family system (e.g. your email provider is part of this system, and you may have other companies involved, as well.)

You'll then examine each resource for its informational burden – how critical is the information that each resource handles? Then you'll also look at how healthfully the resource handles its burden – is each resource supported in the ways it needs to securely carry its burden? For example, you may have a computer that carries a huge burden of client records and emails. Do you support it by keeping it physically safe? Do you load it with software that protects it from viruses or encrypts it so that its information is safe from prying eyes?

For each kind of resource, we supply you with worksheets that contain specific, unambiguous guides for answering those questions.

As you work these worksheets, you'll start to accumulate a list of what we call "risks." These risks will be ranked on a scale of "Low," "Medium," or "High." Risks can look rather like this:

1. Theft of my smart phone can lead to a confidentiality breach of all my text messages and emails. Risk Level: Med.
    - This one would be medium because in your risk analysis, you discovered that you have a lot of good support for your phone to keep bad guys out. But given the informational burden this phone is carrying, you still need to give it a little bit more so the risk goes down to "Low." We'll do that in the Risk Management Plan phase ***(Book 2, coming by Summer 2015)***.
2. Computer virus infection of my computer can damage the computer, and cause me to lose all my client records. Risk Level: High.

- It looks like in this case, the computer is highly burdened with information and poorly supported to keep that information secure. We need to do several things to help keep this computer's information safe in the Risk Management Plan phase ***(Book 2, coming by Summer 2015)***. The workbook will take you through the steps of how to do that.

3. A bad guy can get into my file cabinet and find clients' sensitive information. Risk Level: Low.
    - It looks like even though this file cabinet is probably burdened with a lot of sensitive information, it is well enough supported (probably with a lot of locking doors) to keep bad guys at bay. During the Risk Management Plan phase ***(Book 2, coming by Summer 2015)***, we'll leave this one as-is.

The end result of this process is documentation of your good work and a list of risks prioritized from high to low. We'll use that list of risks in the next phase.

2) Risk Management Plan *(AKA Book 2, coming by Summer 2015)*

Your Risk Management Plan will start with a process of examining your list of High and Med risks and deciding on plans for how to bring those risk levels down.

This workbook will provide a lot of suggestions based on your risk analysis, but sometimes this phase can benefit from some creativity that the workbook may not provide. For example, perhaps with your new perspective on the whole picture of your practice you'll realize it's time to retire some of your resources or that it's time to move your records to "The Cloud."

Or perhaps you'll just change some settings on your computer, move something to a different room, and be done.

It's difficult to predict what this phase will reveal until you reach it.

Based on your needs, the workbook will help you decide what changes you need to make and which Security Policies you need to adopt. You will then set a timeline for putting these changes into effect – probably over the next several months – and be ready for the next phase.

3) Policies and Plans *(AKA Book 3, coming by Fall 2015)*

This is what I like to call the action phase. This is the one where you'll build a set of your security plans based on the template Security Policies provided by this workbook.

The workbook will provide templates for you to build:

- A catalog of your resources. This catalog is where you'll keep track of your security plans, and also you'll keep track of your progress on putting your Risk Management Plan into action.
- A schedule of security tasks. Any good security plan requires maintenance, and this handy schedule will help you keep on task.
- A log of security activities. As my clinical supervisor always told me: document your good work. This is where you'll log all those wonderful things you're doing to

support your resources in their information-keeping burdens and to keep your clients and your practice safe.

The workbook will also provide Security Policies, built with the small mental health practice in mind, to use in your official Policies and Plans manual for HIPAA Security Rule compliance.