SMS IT Group

www.smsitgroup.com

213.222.5182

Written by Scott G. McCarthy

sgm@smsitgroup.com

Business Owner's Guide to HIPAA

Revision 2, September 2014

Revision Notes V2

- Fixed general spelling and grammatical errors
- Added section with greater detail for those interested in handling HIPAA themselves
- Added HIPAA links and 3 step process to start HIPAA plan
- Enhanced PDF version of document
- Added additional information throughout the document based on revision 1 feedback

SMS IT Group
www.smsitgroup.com

Business Owner's Guide to HIPAA

Everything You Need to Know About HIPAA Compliance

About the author: *Scott G. McCarthy is the Director of SMS IT Group in Los Angeles, CA. Mr. McCarthy has been performing PCI and HIPAA audits for well over 9 years. He has a 100% pass rate and has never failed an audit to date. Mr. McCarthy has worked with everyone from small doctors' offices, Fortune 500 Corporations, and law firms. He has successfully passed PCI audits for both law firms and corporations and some of the world's largest banks. Mr. McCarthy can be reached at sgm@smsitgroup.com or at the SMS IT Group at 213-222-5182.*

Why Is HIPAA Such A Big Deal? Why Should I Care?

For those in the medical field, HIPAA remains one of the most confusing and unclear requirements that exist. If you are a larger practice or firm, chances are you have someone in house who is a HIPAA expert or knows enough to get you through filling out the form. For the rest of you, don't make a best effort guess at answering the HIPAA form and drop it in the mail because the consequences can be painful. Even if you never received or had to fill out the HIPAA form, if you store or send electronic patient records, you are required to have a HIPAA plan and follow it!

The best analogy I can use to explain HIPAA is your taxes. Every year, you are required to fill out tax forms whether it be electronically or via paper and submit or mail them in. The government gives you the leniency to fill in your answers as you see fit and works on somewhat of an honors system for the most part. In the event an IRS auditor comes knocking, you better have answered correctly and honestly.

The same principles apply to HIPAA. For the most part, anyone who falls under HIPAA will be required to fill out a form and drop it in the mail back to the government. What most people don't realize is what happens if you get flagged for a HIPAA audit. Just like the IRS, the government audits HIPAA forms and your answers you put on the form. The key difference is that the government usually outsources audits to private companies; and that is bad news! Why you ask? Because the companies they hire are extremely efficient at auditing you and can tell very quickly if you truly comply with the answers you gave on your form. And chances are pretty good you are going to get audited at some point.

Keep in mind the 1st thing the auditor will ask you for is your HIPAA plan for that year and if you can't produce it, you are already in hot water. And no, you cannot retroactively write your plan because the auditor is going to want proof your plan was written on the time and date it was due to be completed.

I Never Worried About HIPAA Years Ago!

You see the government is putting quite a bit of resource into ensuring businesses comply with HIPAA and they are taking it very seriously. I cannot count how many times I get a phone call at SMS IT Group with a panicked doctor on the other end of the phone telling me they have been a target of a HIPAA audit and he wasn't really paying attention when he filled out the form. And oh, by the way, if he doesn't comply, he owes $300,000 immediately due in 30 days. Then the next question I get is "how do I get out of paying this penalty? I didn't realize what I was filling out! HELP!" Sometimes we can get the penalty removed and sometimes they are stuck paying it. It all depends on what they filled out on that HIPAA form and threw in the mail a year ago.

The bottom line is if you transmit health information in electronic form (and that includes email), you probably fall under HIPAA. This rule doesn't only apply to doctors or medical firms, it also applies to law firms and the third party companies that serve them. An excellent example of this is ABC law firm who has a thriving Healthcare Practice that represents 2 dozen doctors and exchanges files with the doctors they represent regularly. Not only is the doctor required to be HIPAA compliant, so is the law firm.

You Better Care About HIPAA If You Want To Keep You Money!

Even if you haven't received the questionnaire or been required to return a HIPAA form, if you handle and send electronic records, you have to be HIPAA compliant. **It is your responsibility to know this and the government is not going to have any pity on you if you plead ignorance.** Even worse, if you are a business that falls under HIPAA and have a records breach meaning that you lost control of your records, someone stole your records, or any event took place in which an unauthorized party gets a hold of your records – even 1 record – the fines are enormous. Take a look at my HIPAA chart below that documents the fines you are required to pay in the event of a breach:

Civil monetary penalties

Tier	Penalty
1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100-$50,000 for each violation, up to a maximum of **$1.5 million** for identical provisions during a calendar year
2. The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.	$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

Yes, if you were paying attention to the chart I provided you can be fined up to $1.5 million in the same calendar year. You are thinking that I am fear mongering and blowing this whole thing out of proportion right? WRONG!

A Real World Example

Let me give you an example. Let's say you are a dentist that does everything right, has extremely happy clients and are a thriving practice. You keep you patient records in your purchased software package that is hosted by the latest wiz bang medical cloud provider. So you think, I am safe because wiz bang provider is responsible for securing my data. So let's then imagine your office administrator runs a patient report for marketing purposes and saves all your patient data into her spreadsheet program on her computer. Since she has never been HIPAA training, she emails out the list to you to review over the weekend. Well, since your Gmail password hasn't been changed in 5 years, Hacker X gets into your account and downloads the list. Hacker x logs into the underground information market and sells you patient list for a cool and quick $10,000. The next thing you know a HIPAA representative is standing in your lobby telling you that your patient records are all over the Internet. And by the way, they want to see your HIPAA compliance plan.

You tell the HIPAA representative that you didn't know you needed a plan and didn't know you needed to do all this to be HIPAA compliant. Can you guess what is coming next? A huge fine! You see every patient record that is compromised; let's imagine there were 5,000 patient records on that report your office manager emailed out; is considered a violation by the HIPAA auditor on a bad day after his wife had him sleep on the couch last night.

This situation is considered "willful negligence" according to our fines chart so let's do the math:

$50,000 x 5,000 patient records = $250,000,000 million

But luckily the good folks at the HIPAA compliance department capped the fines at $1.5 million so you only need to cut a check for $1,500,000. That's a deal, right? I don't know about you but $1,500,000 is A LOT of money to me and to most people out there and not something I want to hand over to anyone anytime soon. Do you get where this is going?

So You Have No Interest Paying $1,500,000

HIPAA compliance is the responsibility of everyone, and I mean everyone, who stores and transmits electronic patient records. I cannot state this enough. Unless you still use an abacus and store everything on paper because you think the computer overlords are going to take over the planet, then you probably fall under HIPAA. And I will say it again – ignorance doesn't work!

And if you still think I am fear mongering, I will give you one more example. I recently was called out to a large practice in Los Angeles after the doctor who owned the practice received one of those *you better be compliant or you have to pay a massive fine letters.* The doctor checked the box that said "I have a completed HIPAA plan for 2013". The problem is he didn't. He was just trying to blow through the paperwork to move on with his life. Well, in 2014, the auditors showed up and asked him for a copy of his 2013 plan. And that's when I got the call asking what he should do. The auditors also told him that if he didn't have the plan and incorrectly filed out the form, he was going to have to write a check to give back all his Medicare subsidies. Let's just say it was a lot of money. Enough to make him sweat profusely.

How About a Vacation to Our Wonderful Federal Institutions?

Not only does HIPAA have civil penalties, it also has criminal penalties just in case you thought of falsifying your forms, lying to the auditors or any other combination of illegal activities to get around HIPAA compliance. You simply don't falsify HIPAA information unless you want to take a free vacation to the United States Federal Prison System. Let's take a look at the criminal penalties involved:

Criminal penalties

Tier	Potential jail sentence
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

Again, HIPAA is just like the IRS. No one ever comes out looking good when they fail to pay their taxes and get audited. The same rule applies to people who simply ignore HIPAA and get caught. I know the entire concept of HIPAA compliance is fairly new but it is time to wake up and pay attention because this act can have massive consequences to your practice and your profits. Ignorance doesn't work anymore.

Still Think I Am a Fear Monger?

So you are reading all this and you still think I am full of hot air or trying to scare the living you know what out of you to earn your business because SMS IT Group obviously handles HIPAA. Well, of course we don't mind your business, however, the point of this article is to educate you and wake you up if you don't yet have a HIPAA plan in place. Just so I put the fear mongering doubt to rest in your head once and for all, let's take a look at the list of HIPAA fines taken right from the www.hhs.gov website. I even included the links so you can read about each case in detail if you want. I want you to pay particular attention to the dates these fines took place:

- $800,000 HIPAA Settlement in Medical Records Dumping Case - June 23, 2014
- Data Breach Results in $4.8 Million HIPAA Settlements - May 7, 2014
- Concentra Settles HIPAA Case for $1,725,220 - April 22, 2014
- QCA Settles HIPAA Case for $250,000 – April 22, 2014
- County Government Settles Potential HIPAA Violations - March 7, 2014
- Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts - December 20, 2013
- HHS Settles with Health Plan in Photocopier Breach Case - August 14, 2013
- WellPoint Settles HIPAA Security Case for $1,700,000 - July 11, 2013
- Shasta Regional Medical Center Settles HIPAA Privacy Case for $275,000 - June 13, 2013
- Idaho State University Settles HIPAA Security Case for $400,000 - May 21, 2013
- HHS announces first HIPAA breach settlement involving less than 500 patients - December 31, 2012
- Massachusetts Provider Settles HIPAA Case for $1.5 Million – September 17, 2012
- Alaska DHSS Settles HIPAA Security Case for $1,700,000 – June 26, 2012
- HHS Settles Case with Phoenix Cardiac Surgery for Lack of HIPAA Safeguards - April 13, 2012
- HHS settles HIPAA case with BCBST for $1.5 million - March 13, 2012

- Resolution Agreement with the University of California at Los Angeles Health System - July 6, 2011
- Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc. - February 14, 2011
- Civil Money Penalty issued to Cignet Health of Prince George's County, MD - February 4, 2011
- Resolution Agreement with Management Services Organization Washington, Inc. - December 13, 2010
- Resolution Agreement with Rite Aid Corporation - July 27, 2010
- Resolution Agreement with CVS Pharmacy, Inc. - January 16, 2009
- Resolution Agreement with Providence Health & Services - July 16, 2008

Are we past the fear mongering doubt now? Do you finally believe HIPAA is the real deal? Good! Truth be told that if you follow the rules and this article, HIPAA is not overly complex nor should be that scary. You just need a plan to ensure you never see a HIPAA fine. Let's get into handling HIPAA and making sure you are protected.

I'm Convinced! Now What Do I Do?

So I think we are finally ready to discuss what you should do and how you should handle HIPAA. I am going to assume you are a business that stores or transmits electronic patient records for the purpose of this discussion. According to HIPAA guidelines and standards, you need a plan and this is where most people get lost. The problem with HIPAA, as well intentioned as it is, is that it's very vague and applies to so many different entities that it's almost impossible for the government to make it specific. HIPAA covers the 2 person doctor's office all the way to the 5,000 attorney law firm and when you have that much range, the parameters are going to be vague.

That's where people like me come into play. Consultants such as myself know how to read the guidelines and apply them to your business. I have a strong knowledge of IT, HIPAA, office procedure, security and other elements that afford me the capacity to properly interpret the rules and apply them to the business I am dealing with. I take the HIPAA guidelines, complete an analysis of your business and deliver to you a completed plan that covers you. If you don't want to understand anymore, just pick up the phone, give me a call, and I will make you compliant. My information is at the top of this document. Otherwise, if you want to handle HIPAA yourself or understand more about how HIPAA works, keep reading.

Like I said, each business needs a plan but it takes a lot of work and knowledge to get that plan together. I just can't sit down and write a plan and deliver it to you. How easy would that be! If you want to get a HIPAA plan together, you must first survey your business. You must look at how your staff works, how your IT systems are setup and all the security precautions missing and in place. Then, you must compare your information to the HIPAA guidelines and come to a conclusion as to which areas you are deficient. If this is your 1st plan, you are going to be deficient in every area.

After you identify where your deficiencies lye, you need a plan to correct them. The next step is to correct each deficient area and ensure your correction complies properly with the HIPAA requirement. This is where it gets tricky. Remember how I told you that HIPAA covers a wide range of businesses? The result is very broad HIPAA open to interpretation by you and the auditors. This is where HIPAA gets really tricky and why I strongly recommend you hire someone with HIPAA experience to help you – even

if you don't hire me (joking). Many of the deficiencies will require a high level of IT experience. Let me give you an example.

HIPAA requires that data that leaves your business encrypted. Email is an example. Regular email transmission is unencrypted. When your staff attaches a document that contains patient information and clicks send, you have just sent unencrypted information and violated HIPAA. The trick is having enough IT knowledge to replace regular email with an encrypted solution. You see how this is pretty involved?

Not only do you have to correct each deficiency with a solution, you need to train your staff on how to use the new procedures and make sure they comply every day. I recommend assigning someone with authority such as the office manager to ensure your employees follow the new procedures until they become second nature. After that, you need to keep logs and record ongoing information. Let's look at another requirement, shall we?

One of HIPAA's requirements is to keep a facilities log of any vendor or third party who enters your office and potentially has access to your patient information. Someone in your organization needs to keep a log and be able to show this log as part of your HIPAA plan each year. If not, you don't comply. You need to actively involve your staff in the new HIPAA procedures. Once you complete your HIPAA plan, you must follow it every day.

Theoretically, let's say you go through all the requirements and complete your plan. You retrain your staff, put new procedures in place, dole out new responsibilities, hold a training session and file your plan away. Not so fast! You have to follow what you documented in your plan all year long. What most people fail to realize is that HIPAA is a living and breathing document. It's not something you write and throw in the drawer for a year. It has to be followed and if it's not, it's a breach. Get ready to pay some fines.

It is true that auditors are generally more lenient with businesses that have made an attempt to write a plan and comply with it; but they can still fine you. When next year rolls around and the requirements are updated or you need to update your plan because your business processes have changed, it is much easier to do so if you follow your plan and modify it through the year. I highly recommend someone in your organization take responsibility for your plan. Someone should be compensated and given the responsibility to be the HIPAA enforcer. Actually, that's what HIPAA requires anyway so it's better just to do it.

MY HIPAA Recommendations

There is no doubt that given the right money, time and dedication, anyone can follow HIPAA. But that's the problem. Most people don't have the time to learn it well enough and make sure their business is compliant. You can become a corporate tax specialist as well but why? I highly recommend you hire someone with a high level of knowledge who has passed at least one HIPAA audit to help write your plan and make your business compliant. Even if you think you did a good job handling your HIPAA compliance in house, you will never know unless something happens or the auditors show up. Given the fines, it's not a risk I would be willing to take.

I compare those who try to write their own HIPAA plans to an individual trying to sit down and file your own S-Corporation reports while managing the accounting and filing your corporate taxes. Most every

business has a tax expert look over its filings and HIPAA should be no different. I cannot stress enough that each business should hire an expert to handle HIPAA. Not only should you hire the expert, you should give that person enough power to execute the plan and properly train your staff. When your HIPAA consultant gives you recommendations, follow them. Make them the gospel of your business and make sure your employees understand how important HIPAA is. Lead by example.

Don't handle HIPAA yourself unless you have an employee who is extremely experienced with IT that has some level or HIPAA or PCI knowledge and has done it before. The stakes are just too high to do it differently.

I Want To Do It Myself – Or Make An Attempt – How Do I Do It?

STEP 1:

The 1st thing to do is determine if you truly fall under HIPAA. You can go through a quick **questionnaire** at http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html. This will give you a good idea if you are required to comply or not. Go through these questions and if you fall under HIPAA, keep reading.

STEP 2:

Let's say you are dead set on hiring someone to help you which I strongly recommend. No problem – I have no issues telling you how to accomplish it. The **HIPAA *Summary of the Security Rules*** can be found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html. The government provides this as a guide to all the HIPAA requirements and what you need to comply with whether you are a 5,000 person corporation or 2 person doctor's office.

STEP 3:

To start, you need to read through this web page which is designed as a starting point for HIPAA compliance http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.

STEP 4:

Once you are done reading through the introduction, you then move on to http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html which covers specific items you need to ensure you comply with. This is the web page you can use to build your HIPAA plan from. This is probably the most important web page as you use this to read through each requirement and compare your office procedures to the HIPAA rules. The rules are broken into subsections and each link covers specific sections of the HIPAA requirements. For example, *physical safeguards* is a sub-section that covers how to comply with the physical office requirements of HIPAA.

Now remember that HIPAA is completely subjective and open for interpretation so there is no magic formula I can provide to tell you how to handle it for every single company out there. If I could put a 3 step guide together, I wouldn't be consulting and helping people with HIPAA but unfortunately it's not that simple. What you can do is read through each step (1-3) with the links I documented. Then, come up with a plan on how to comply for your organization and start to build that plan. There is no right or wrong way to accomplish it as long as you meet the guidelines.

So let's go back to physical safeguards. You can go into that section and come up with a plan to meet those requirements for your business. Document where you are at now, what you need to change, how you are going to change it and then change it. Train your staff on the new requirements and make sure everyone complies. I use physical safeguards as an example because it's a fairly easy and straightforward section to start with.

You can use the steps above to start to build your plan. Remember that the plan is just the beginning. You still need to be prepared for an audit, train your staff, and know how to handle breaches, etc. My point is that HIPAA is very involved and if you are determined to take it on, you are going to have to learn everything about it and become an expert to make sure you don't put your organization in danger. It is absolutely possible that if you put in the time and dedication you can learn it. But, again, with so much at stake, one mistake can cost you dearly.

Although everything is laid out on the links I provided, I strongly, strongly, strongly urge you to hire a consultant or professional. HIPAA has so many twists and turns it is almost the same thing as saying I am going to pick up this corporate tax guide and become a corporate tax professional. Sure, if I put my mind to it, I probably can become a corporate tax professional. Let's hope I don't make a mistake on my 1st filing.

Again, if you are determined to do it, go through the links above and read everything and formulate a plan in your head on how you can make it work for your business. Just remember that HIPAA is completely subjective and there is no right or wrong way to handle it as long as you comply with the rules. The auditors don't care how you do it as long as your plan can be followed, your staff follows it and you meet each rule in the HIPAA parameters.

It is important that your plan is clear and easy to read and it closely follows every rule in the HIPAA guidelines. Also keep in mind that HIPAA changes quite often so you are going to need to keep up with changes in HIPAA to make sure your plan complies on an ongoing basis. HIPAA was and is designed to be an ongoing effort to protect patient's data and not a one-time effort.

I wish I can give you a step by step process but this is where it gets murky. If you are determined to tackle HIPAA on your own, the best advice I can give is to read through all the links I provided and devise a plan that matches your business. Build the plan to the best of your ability and make sure that at the end of the day, you have complied with each HIPAA requirement.

I cannot overstate enough how much I recommend hiring a professional as I have been called in many times to bail out a company that has screwed up a self-written plan. Also remember that even if you are able to understand HIPAA completely, writing a plan and complying is a full time job. It can take over 1-6 months to put in place depending on the complexity of your company and how much needs to be fixed. You will have to do your regular job and HIPAA as well.

OK. I'm Convinced That I Need to Hire Someone to Help

When you look for a consultant to help with HIPAA, don't go cheap! Remember how much the HIPAA fines were? OK! Don't hire the guy that fixes your PCs or a relative. Hire a professional with a track record! Would you hire a barber to handle your taxes?

Look for someone who can provide references and show proof of work. In some cases, references might be tough because people get a little sensitive about discussing HIPAA. I know I have trouble asking my past clients for a reference because the stakes are so high. Ask to see samples of their work. Their HPPA plan should look professional, detailed, clean and easy to read. When you look at the samples, think of yourself as the auditor and if the work would impress you.

The plan should have detailed diagrams showing your workflow, tables showing your applications, documents diagraming your staff, and so on. The plan should show each HIPAA requirement listed and the status before and after the plan was written. It should have remediation details and a table of contents. Ask the person to show you a couple examples of HIPAA requirements and then the corresponding plan entry.

Negotiate with the consultant to make sure you pass and ask if you will pass. If not, ask why. If you have done something wrong, there is a good chance you won't pass. Ask what your odds are of passing. Also ask the consultant how he is going to approach your situation if you are facing a fine or audit. Even with all these questions, the golden rule is a track record. Look for someone who was highly recommended to you and has passed HIPAA audits before.

I wish you good luck and hope you the best in your endeavors to comply with HIPAA.