



Petronella  
TECHNOLOGY GROUP

# HIPAA System Blueprint


Get HIPAA Compliant in a few months!



# Table of Contents

Petronella & HIPAA Introduction .....	3
What is HIPAA? .....	4
Petronella - 4 Pillars Risk Assessment .....	28
12 Month Service Introduction .....	34
Month 1: Regulatory Compliance .....	35
Month 2: What Does it Take to Comply With HIPAA? .....	37
Month 3: Jobs to Be Done .....	38
Month 4: Security Controls .....	41
Month 5: Important Policies and Procedures .....	44
Month 6: HIPAA Security Awareness Training .....	45
Month 7: HIPAA Training Continued .....	46
Month 8: Risk Assessment Overview .....	47
Month 9: Compliance Services .....	48
Month 10: Remediation .....	51
Month 11: Remediation Continued .....	52
Month 12: HIPAA Compliant and Peace of Mind .....	53
Customer Reviews .....	54
HIPAA Store .....	55
Petronella Service Agreement .....	56


# Petronella & HIPAA Introduction



Petronella Technology Group knows HIPAA. It's a confusing maze, but we've made it to the other side. We now offer a COMPLETE solution to HIPAA compliance- and we guarantee to get you there in 12 months. Run from anyone who says they can get you there right away. They don't understand the layered nature of HIPAA, and they will lead you to disaster. To do something right, you must take it layer by layer. You must incorporate all the layers into one pretty picture- it is a process. Once one layer is cleared it opens the door to the next layer, and that is how you weave yourself through the maze and live to tell about it. We do offer a la carte solutions, but you would be wise to completely tackle HIPAA head-on. Or should we say, let us tackle HIPAA for you. Let's take a look at why it's the best route to take...

# What Is HIPAA?

## Learn the HIPAA Maze In Minutes!



HIPAA is the “Health Insurance Portability And Accountability Act of 1996,” signed into law by President Bill Clinton after Congress approved the Bill. With HIPAA, very little is clear; in fact, we’ve been living in the gray area since 1996! It brought on the gray era in regard to cyber space, privacy, electronic information, data, archived records, protected health information, digital documents, Federal Rule enforcement, cyber defenses, new systems of Rule, and the advances of high technology. HIPAA may be the one topic that continues to cause insomnia for even the most sleep deprived health professionals, and all of their business associates. It is complicated, it is complex, it is controversial, and it is cumbersome. It’s a tangled web, but we can help unravel it. Let’s start with the good news—you’ve walked through our digital doorway! If HIPAA were a desert, we’d be an underground oasis serving cold water that’s been filtered by reverse osmosis- on tap, with little umbrellas on top. We are known for producing solar flares in the virtual reality, releasing the forces of the Internet that are buried under congested pathways of misinformation. Petronella Technology Group is home to CEO Craig Petronella, a real-life fountain of HIPAA wisdom. Craig serves as Fractional Chief Information Officer (CIO) and Fractional Chief Information Security Compliance Officer (CISCO) for many small and mid-sized organizations. He’s the Amazon best-selling author of “How HIPAA Can Crush Your Medical Practice,” as well as books on cybersecurity, hackers, and computer malware. Next one is on the potential nemesis of HIPAA: the unification of blockchain and artificial intelligence (much more on that below). That’s our Ace Card, played upfront! We are huge fans of total transparency. Not following? Let’s explore the dark alleys of HIPAA Compliance for a moment-

# What Is HIPAA?

don't worry, we are known for turning on the lights. When we emerge at the end of the tunnel, you will see a completely different picture- and dusk will have turned to dawn.

## Let's Reverse Engineer HIPAA

Have you ever read terms and conditions forbidding reverse engineering? That's too bad, because it is so fun. Let's start at the beginning. We've written a very happy ending, but we won't deprive you of an old-fashioned dramatic story line. Besides, isn't the journey the reward? Okay, maybe not for the medical practice here in Raleigh, North Carolina that was recently fined \$750,000 for a single HIPAA violation (and some would argue, a minor one). But you know what we mean. Give us two minutes, and we will give you HIPAA in sixty seconds. With the extra minute, we will summarize the state of the world for you. We'll tell you what everyone has gotten all wrong, and why we've got the Ace Card.

## HIPAA Actuals and Factuals:

### Health Insurance Portability and Accountability Act of 1996

PUBLIC LAW 104-191104th Congress An Act To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, SECTION 1. SHORT TITLE; TABLE OF CONTENTS.(a) SHORT TITLE.—This Act may be cited as the “Health Insurance Portability and Accountability Act of 1996”.(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows: Sec. 1. Short title; table of contents. TITLE I—HEALTH CARE ACCESS, PORTABILITY, AND RENEWABILITY



# What Is HIPAA?

## But Wait, There's More...

If you go to [www.hhs.gov](http://www.hhs.gov), you'll find the U.S. Department of Health and Human Services. They've put together a "Combined Regulation Text," in the form of a PDF. From [www.hhs.gov](http://www.hhs.gov): "This is an unofficial version that presents all the HIPAA regulatory standards in one document." And it's 115 pages long, we might add. Did we mention that it's the unofficial version? Now that you understand this, we should tell you that...well...there's still more. You should review the "Final Privacy Rule" of 2000, which was later amended in 2002. Compliance with this Rule has been required since 2003. Next, there is the "Final Security Rule" of 2003- compliance with this Rule has been required since 2005. In a nutshell, "this Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information." This is where people are going so, so wrong. But we'll get back to that when we move on to minute number two. For now, there's twenty more seconds of pure federal regulatory fun. You guessed it...there's more! Next, there's the "Enforcement Rule" that provides standards for the enforcement of all the "Administrative Simplification Rules." Moving along to the "Final Omnibus Rule" that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the "Breach Notification Rule." Did you notice that we slipped the "HITECH Act" in there? What is HITECH, you ask? From [www.hhs.gov](http://www.hhs.gov): "The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law by Barack Obama on February 17, 2009, to promote the adoption and meaningful use of health information technology." It's HIPAA's commandeering companion, and those who find themselves buried under its many tentacles of EHR systems are trapped. Those who ignore it have built their houses out of a stack of floppy, wet thumb drives that are plugged into a system USB drive, and linked to a malware-infected UPS (Uninterruptible Power Supply), stored in the internal storage of a corrupted and congested system. Bad. It's real bad.

# What Is HIPAA?

## Office of Civil Rights Letter



**DEPARTMENT OF HEALTH & HUMAN SERVICES**  
Office of the Secretary

Office of the Regional Manager  
Office for Civil Rights  
1961 Stout Street, Room 08.148  
Denver, Colorado 80294

Voice: (303) 844-7915  
TDD: (303) 844-3439  
Fax: (303) 844-2025  
Website: [www.hhs.gov/ocr](http://www.hhs.gov/ocr)

JUN 27 2016

Re: [REDACTED]

Dear [REDACTED]

Please be advised that, on February 16, 2016, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), received a complaint from [REDACTED] alleging that [REDACTED] may not be in compliance with the applicable provisions of the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 Code of Federal Regulations (C.F.R.) Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules) and the Breach Notification Rule (45 C.F.R. Parts 160 and 164, Subpart D).

Specifically, Complainant alleges that on February 3, 2016, [REDACTED] was burglarized, and three computers and a mobile storage device were stolen that contained electronic protected health information (ePHI). Complainant further alleges that the passwords and "key" for the ePHI was stolen with the devices. Additionally, she alleges she advised [REDACTED] managers of their obligation to notify HHS and affected individuals, but they did not do so. On February 12, 2016, [REDACTED] terminated Complainant's employment with it, which she alleges was in retaliation for her advice to handle the theft as a breach under the Breach Notification Rule and make notifications. These allegations indicate potential violations of 45 C.F.R. §§ 164.308(a)(1)(ii)(A) (Risk

Analysis), 164.308(a)(1)(ii)(B) (Risk Management), 164.308(a)(5)(D) (Password management), 164.308(a)(6)(ii) (Response and Reporting), 164.310(a)(1) (Facility Access Controls), 164.310(a)(2)(ii) (Facility Security Plan), 164.310(c) (Workstation Security), 164.312(a)(2)(iv) (Encryption and Decryption), 164.312(d) (Person or Entity Authentication), 164.404(a), (b), (c), (d) (Breach notification to individuals), 164.408(a), (b) (Breach notification to the Secretary), 164.502(a) (uses and disclosures), and 164.530(c) (safeguards), (f) (mitigation), and (g) (refraining from retaliatory acts).

OCR enforces the Privacy and Security Rules, and the Breach Notification Rule. OCR also enforces Federal civil rights laws that prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and, under certain circumstances, sex, and religion.

OCR is responsible for enforcing the Privacy and Security Rules as they apply to "covered entities" and "business associates." Covered entities are health care clearinghouses, health plans, and health care providers that transmit health information in electronic form in connection with a transaction for which HHS has adopted standards. See 45 C.F.R. Part 162. Business associates are persons or entities that provide certain services to or perform functions on behalf of covered entities, or other business associates of covered entities, that require access to protected health information.



# What Is HIPAA?

## Office of Civil Rights Letter

To learn more about what types of entities are covered entities and business associates, please go to <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>. You can also find helpful information about the Privacy and Security Rules at OCR's website, <http://www.hhs.gov/ocr/hipaa>. Among other things, the website provides a summary of the Privacy and Security Rules, guidance and fact sheets about the Privacy and Security Rules, HIPAA training materials, sample notices of privacy practices and business associate agreements, and answers to hundreds of frequently asked questions. If you do not have access to the Internet, you may also obtain additional information and request a summary of the Privacy and Security Rules by calling the investigator identified at the end of this letter.

Our authority to collect information and ascertain a covered entity's or business associate's compliance is found at 45 C.F.R. §§ 160.300 - 160.316. These provisions give OCR specific authority to investigate complaints and conduct compliance reviews. Covered entities and business associates must cooperate with OCR during a complaint investigation or compliance review (45 C.F.R. § 160.310(b)) and permit OCR access to its facilities, records and notice, if exigent circumstances exist (45 C.F.R. § 160.310(c)). To the extent practicable, OCR will seek the cooperation of covered entities and business associates to informally resolve complaints. For example, OCR can provide technical assistance to help a covered entity or business associate voluntarily comply with the applicable provisions of the Privacy and Security Rules. We have attached a list of needed data and information and request that you submit your responses to us **within 14 days of the date of this letter**. Please number each response to correspond with the number in the data request.

A covered entity or business associate has the right to respond to an allegation by submitting evidence to OCR indicating: it is not a covered entity or business associate subject to the applicable provisions of the Privacy and Security Rules; the alleged violation did not occur as described by the complainant; the action complied with the Privacy and Security Rules; or the covered entity or business associate has taken prompt and effective action to correct the noncompliance.

If we are unable to resolve this matter voluntarily, and if OCR's investigation results in a finding that [REDACTED] not complying with the Privacy or Security Rules, HHS may initiate formal enforcement action which may result in the imposition of civil money penalties. We have enclosed a separate fact sheet explaining the penalty provisions under the Privacy and Security Rules. The fact sheet also explains that certain violations of the Privacy and Security Rules may be subject to criminal penalties, which the U.S. Department of Justice is responsible for enforcing.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

Please be assured that our office is committed to resolving this matter in an efficient and timely manner. If you have any questions, please do not hesitate to contact Karel Hadacek, J.D., Equal Opportunity Specialist, at (303) 844-7836, or via email at [karel.hadacek@hhs.gov](mailto:karel.hadacek@hhs.gov). When contacting this office, please remember to include the transaction number that we have given this file. That number is located in the subject line of this letter.

Sincerely,



Andrea Oliver  
Regional Manager

Enclosures: Data Request  
The Privacy and Security Rules Enforcement and Penalty  
Provisions Fact Sheet



# What Is HIPAA?

## Office of Civil Rights Letter

### DATA REQUEST

████████████████████

Please provide OCR the information requested below to demonstrate ██████ compliance with the Privacy, Security, and Breach Notification Rules. If such documentation is not provided, OCR will conclude that it does not exist. Please provide the following information to OCR, numbering each item in your response to correspond with the requested item:

1. ██████ position regarding the allegations.
2. a copy of the most recent risk analysis performed for or by ██████ to identify potential risks and vulnerabilities (with appropriate risk level) to logical, physical and network security of the systems that store or contain ePHI. See 45 C.F.R. § 164.308(a)(1)(ii)(A).
3. the risk management plan, policies, and procedures used by ██████ to implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level, based on the risk analysis. Include evidence of completed risk remediation actions. See 45 C.F.R. § 164.308(a)(1)(ii)(B).
4. evidence of password management for ██████ computers and mobile storage devices. Please provide the password management policies including the password length, password age and password complexity requirements and evidence that ██████ staff have been trained regarding the procedures. See 45 C.F.R. § 164.308(a)(5)(ii)(D).
5. documentation and outcome of any investigation ██████ conducted into the theft of its computers and mobile storage device, including a description of the breach, incident report, corrective actions taken, and mitigation taken. See 45 C.F.R. §§ 164.308(a)(6)(i) and (ii).
6. if ██████ made a report to local law enforcement, provide a copy of the agency's investigation report. See 45 C.F.R. §§ 164.308(a)(6)(i) and (ii).
7. evidence of the implemented policies and procedures and access controls in place to limit physical access to ██████ electronic information systems and the facility or facilities in which they are housed. See 45 C.F.R. § 164.310(a)(1).

This is an OCR audit letter that will make you cringe. Be proactive! Be prepared and be able to respond confidently that your practice CAN pass an audit with flying colors.

## Sixty Seconds/Second Half

So we didn't call it bad news, but you probably realize that we just gave it to you. But remember the good news- you're here, and it's all about who you know. And the cards you are dealt. In this case,

# What Is HIPAA?

remember our Ace Card? We pointed out that the “Final Security Rule” was where people were going really wrong. Or should we say, the wrongest?

ALL of the Rules are bringing out the worst in everyone, and we’ve worked with many practices that were sincerely trying to be compliant.

Did you know that encryption is not required by HIPAA?

It’s a great service, that’s not actually required. It’s part of the higher end Google G-Suite plans, the paid version of Google services where Google will sign a Business Associate Agreement (BAA) IF and ONLY IF you properly configure the security controls within the Google ecosystem. Otherwise, as defined in their terms and conditions, you can still suffer a breach and/or steep fines! Microsoft has similar HIPAA compliant services in their Microsoft Office 365 E3 packages that include a system called Compliance Manager, which makes adhering to HIPAA regulations easier in the event of an audit. Microsoft will also sign a BAA if you properly configure the HIPAA security controls on the Microsoft Office 365 system through Compliance Manager. Microsoft Compliance Manager is not a simple system to configure properly. I recommend seeking professional services from a reputable and reliable cybersecurity and compliance firm.

Google sure benefits from medical practices that need to comply with HIPAA regulations. But don’t blindly help them. You can actually write into your policies and procedures that email is not a supported communication for your practice. This is an area that we specialize in; instead of using insecure email, we use an “encrypted portal system.” There are different levels with everything, including the

# What Is HIPAA?

internet itself. You'll find the same is true with security in the cyber realm. But remember, the "Final Security Rule" is the Rule that "sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information." Key words: CONFIDENTIALITY, INTEGRITY, AVAILABILITY.

Why are these so key? We live in the Digital Age, and hackers are wreaking havoc. How confidential are your records when a hacker breaches your network? What's the integrity of your electronic health information looking like when you've got hackers browsing through it? How available are your files when they're encrypted with ransomware? We don't like to sugarcoat things. You're on the World Wide Web, and so is your business. You are on their turf, and they know the land far better than you do. They have booby traps and land mines everywhere, and you are a sitting duck. They are master duck hunters. But we know how to glitch their game system.

How many ducks do you remember getting when your virtual duck gun was unplugged?

Do you see how this all comes full circle? Craig Petronella, CEO of Petronella Technology Group, is an international authority on BOTH HIPAA AND CYBERSECURITY. Now that's Wisdom.

You can go elsewhere for help with HIPAA, and as you walk in the other direction you will be getting further and further from the light at the end of the tunnel. May we be blunt? Everything, and we mean EVERYTHING, changed on January 1, 1983. But why, you ask, since HIPAA wasn't enacted until 1996 (ten years after the Internal Revenue Code of 1986)? Because that's when the Internet dropped its web on the whole wide world. We won't sell you a do-it-yourself HIPAA

# What Is HIPAA?

Compliance package for \$250, as some will. They might even be willing to throw in a bottle of snake oil for an extra twenty bucks, and a thermos of their specially brewed kool-aid to quench your thirst for good.

And to cook your goose with the Office of Civil Rights (the auditing arm of HIPAA, between arms 9 and 10 of HIPAA). As you learned in the first sixty seconds, this is a lion's den. And you're trapped inside of it, under a spider's web. We like to speak the truth; forgive us for being so blunt. Even cybersecurity "experts" come to us for help. We are the Bruce Lee of Cybersecurity, and the Bruce Lee of HIPAA. We are Bruce Lee, SQUARED. We are the Thunder, and we are the Lightning, and this is the Perfect Storm.

Yes, the rules of the game have changed. But, we pulled a genius move:

"Learn the rules of the game; then play better than everyone else."  
-Albert Einstein

Learn More About How We Play, So That You Can't Lose.

Perform a HIPAA Security Risk Assessment to score your practice as soon as possible!

Look at what happened to the practice below when they failed to do a HIPAA Security Risk Assessment. A requirement to be done annually as part of the criteria to receive incentives and funding from the government. They got the letter below from the OCR outlining the rejection according to meaningful use terms.



# What Is HIPAA?

## This Is A Redacted Fax of a Meaningful Use Audit Rejection Letter

Comments:

Please see attached.

<input checked="" type="checkbox"/> CMSLogo.jpg	<input checked="" type="checkbox"/> FigliozziLogo.png	<input checked="" type="checkbox"/> EHRLogo.jpg
---	---	---

July 20, 2015

**RE: HITECH EHR Meaningful Use  
Audit Determination Letter**  
**NPI:**  
**Attestation Period: 10/1/2014 - 12/31/2014**  
**Program Year: 2014**  
**Payment Year: 3**

We have completed our audit of how you demonstrated meaningful use of certified Electronic Health Record (EHR) technology in accordance with Section 13411 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), as included in Title XIII, Division A, Health Information Technology and in Title IV of Division B, Medicare and Medicaid Health Information Technology of the American Recovery and Reinvestment Act of 2009. The HITECH Act provides the Secretary, or any person or organization designated by the Secretary, the right to audit and inspect any books and records of any organization eligible to receive an incentive payment.

We performed a review of your meaningful use attestation for the Program Year 2014 and Payment Year 3. Based on our review of the supporting documentation furnished by you, we have determined that you **have not met** the meaningful use criteria, for the following reasons:

- Failed Eligible Professional Meaningful Use Core Measure 14 - Protect Electronic Health Information

Since you did not meet the meaningful use criteria, you will not receive an incentive payment for this program year. We hope that you will be able to make the necessary practice workflow adjustments in order to successfully demonstrate meaningful use next year.



# What Is HIPAA?

## This Is A Redacted Fax of a Meaningful Use Audit Rejection Letter

**HIPAA Security Risk Assessment – [REDACTED]**

Implementation Specification	R/A	Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
<b>Administrative Safeguards</b> Security Management Process 164.308(a)(1) Team: Security Official, Physician, Workforce Members								
Risk Analysis	Required	Do you keep an updated inventory of hardware and software owned by the practice?			✓			
		Can you identify where ePHI is located (e.g., desktops, laptops, handhelds, tablets, removable media, servers, etc.)?			✓			
		Could you locate the inventory in a disaster (fire, flood, explosion, theft)?			✓			
		Do you know the current approximate value of your hardware and software?			✓			
		Does the inventory contain all necessary contact information, including information for workforce members and service providers?			✓			
		Do you control the information contained on your information system?			✓			
		Do you or your workforce take home portable computers or other devices containing ePHI?			✓			
		Does any vendor have access to confidential patient data? Have you			✓			

**HIPAA Security Risk Assessment – [REDACTED]**

Implementation Specification	R/A	Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		discussed HIPAA Security and HITECH requirements with such vendor(s)? Is an up-to-date Business Associate Agreement in place for each vendor that has access to ePHI?						
		Can a vendor change confidential patient data? If so, are you monitoring audit logs for such changes?			✓			
Risk Management	Required	Do you update your workforce members' training each time you develop and implement new policies and procedures? Do you document initial and continuing training?			✓			
		Have you set user access to ePHI? Does access correspond to job descriptions (clinical, administrative, billing)?			✓			
		Do you monitor reports that identify persons and systems that access ePHI, including those not authorized to have access to ePHI?			✓			
		Do you have control over who can amend your patient records?			✓			
Sanctions Policy	Required							

**HIPAA Security Risk Assessment – [REDACTED]**

Implementation Specification	R/A	Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Have you developed a written sanctions policy against workforce members who do not abide by your policies?			✓			
		Have you explained those sanctions to your workforce members?			✓			
		Do you consistently enforce those sanctions?			✓			
Information System Activity Review	Required	Do you regularly review system audit trails that identify who has accessed the system and track additions, deletions, or changes they may have made to ePHI?			✓			
		Would you know if someone was trying to hack into your system? (Do you regularly review security incident reports?)			✓			

# What Is HIPAA?

## What is HIPAA Compliance?

HIPAA compliance is the act of complying with all of the above, and a bit more! Surely you noticed the wording “and other purposes” in the legal description of HIPAA from [www.hhs.gov](http://www.hhs.gov)? There’s quite a bit of that going on. HIPAA compliance is not violating any of the rules- even the vague and unclear ones. When you need your back adjusted, you can ask your 17 year old high-school-wrestler nephew to do it, or you can go to a trained Chiropractor. When you need your car fixed, you can ask your neighbor to do it for you, or you can go to an ASE Certified Mechanic. If you want to be HIPAA compliant, you can do it yourself (correction, you can ATTEMPT to do it yourself- but you won’t be compliant). Or you can call someone who has 1/10 of the experience with HIPAA that we do, with five times the shady marketing budget. Or you can do it right the first time, and then run your practice with the peace of mind you won’t feel otherwise. What does HIPAA Compliance mean? HIPAA compliance means adhering to the Privacy Rule, the Security Rule, the Final Omnibus Rule, HITECH Act. It almost always means involving an expert in your quest for HIPAA compliance, or spending over a decade learning the loosely defined Rules that we already have a grasp of.

## What is HIPAA Law?

The Health Insurance Portability and Accountability Act of 1996 was enacted by the 104th United States Congress and signed by President Bill Clinton in 1996. HIPAA was the catalyst for health information going electronic. It was also the trap for violating privacy and security Rules pertaining to the electronic health records. HITECH added more regulation, and created a big demand for firms that can help with HIPAA, security, privacy, etc. In summary: The Privacy Rule, a Federal



# What Is HIPAA?

law, gives you rights over your health information and sets rules and limits on who can look at and receive your health information. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The Security Rule is a Federal law that requires security for health information in electronic form.

## What is HIPAA Training?

HIPAA requires both covered entities and business associates to provide HIPAA training to members of their staff who handle PHI. Business associates and any of their subcontractors must also be trained. Anyone who comes into contact with protected health information (PHI) must be trained. They need to be trained on Policies and Procedures, and you must also have these in writing! You must have a Sanction Policy that outlines how you will handle staff who violate policies. You can't use generic policy templates and be compliant. They have to be customized for your practice (we do that too). Staff should understand HIPAA very well. We have a staff training program that is more thorough than what you will find elsewhere. In addition, we do training updates regularly. HIPAA is never out of sight with us, and so it's never out of mind. How often is HIPAA training required? The HIPAA training requirements are more guidance than law – suggesting training should be provided periodically and when certain events occur. Again, more vague language. We suggest comprehensive yearly training, with ongoing training on a monthly basis. It wouldn't hurt to throw in weekly “pop quizzes” and “phishing email tests” as a precaution, and we offer these as well. Since the law is vague, the more you do to show due diligence in compliance, the better off you should fare.

# What Is HIPAA?

## All-in-one HIPAA Security Service

*The fastest, easiest and most inexpensive way to HIPAA compliance*

All the tools you need to comply



### Thorough Risk Assessment

- ✓ We perform your Risk Assessment
- ✓ Streamlined Risk Assessment Process - **you will spend around 1 or 2 hours working with us and then we do the rest!**
- ✓ We make additional security recommendations
- ✓ HIPAA Compliance Snapshot
- ✓ Threats Analysis / Risk Determination
- ✓ Remediation / Work Plan
- ✓ **Satisfy Meaningful Use Requirement** - Core Objective - Protect electronic health information (*Conduct or review a security risk assessment of the certified EHR technology*) - **don't put those incentive payments at risk!**
- ✓ Easy to understand reports/work plans



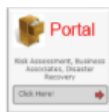
### HIPAA Security Training

- ✓ We train your Employees
- ✓ Interesting and engaging training videos - **HIPAA is boring no more!**
- ✓ HIPAA training for existing and new employees
- ✓ Retrain employees on an annual basis
- ✓ Provide employee compliance testing
- ✓ **View compliance reports that show when employees were trained and their compliance testing scores.**
- ✓ Employee Security Reminders



### HIPAA Policies and Procedures

- ✓ We Write your Policies and Procedures
- ✓ Employee access to policies and procedures
- ✓ Videos explaining security policies
- ✓ Easy to understand policies
- ✓ Easy to follow procedures
- ✓ Addresses the HIPAA Security and Privacy Rules
- ✓ **Allows you to show compliance with HIPAA regulations and protect patient information!**



### HIPAA Compliance Portal

- ✓ **Online access that makes complying with HIPAA easy!**
- ✓ Employee access to policies and procedures
- ✓ Track Business Associates
- ✓ Security incident response
- ✓ Access disaster plans
- ✓ Store contracts and documents
- ✓ HIPAA related information
- ✓ Educational videos
- ✓ Audit "Book of Evidence"



### Easy to Use

- ✓ We do all the hard work for you!
- ✓ **Streamlined Risk Assessment** - only takes around 1 or 2 hours to complete
- ✓ HIPAA Policies are easy to understand and **employees love the policy videos!**
- ✓ **Training is light and enjoyable** - *HIPAA is boring no more!*
- ✓ Our team is with you through the whole process - **we'll get through this together!**
- ✓ Our tools and templates make HIPAA easy!
- ✓ **The price of our service** is easy on your wallet



### \$100,000 Financial Protection

- ✓ **Financial protection from fines and breach expenses!**
- ✓ HIPAA breach related expenses
- ✓ HIPAA violation fines
- ✓ Includes PCI (Credit Card) breach expenses
- ✓ Available to Covered Entities and Business Associates
- ✓ Available for organizations with 50 or fewer employees
- ✓ **Allows you to sleep at night knowing your protected!**
- ✓ [Read More](#)

# What Is HIPAA?



## Security Incident Response

- ✓ Security breaches are stressful – we are here to help!
- ✓ Security Incident Response Tools
- ✓ Required breach Risk Assessment tool
- ✓ Breach documentation tool
- ✓ Patient/HHS notification steps
- ✓ Access to security experts to assist with breach response
- ✓ Our security breach tools combined with financial protection will make a bad situation much better!
- ✓



## Track Business Associates

- ✓ Business Associate tracking tools
- ✓ Business Associate Agreement (BAA) templates
- ✓ Upload BAAs to Compliance Portal
- ✓ Business Associate (BA) compliance verification questionnaire – make sure your BAs are protecting patient information!
- ✓ We help you track Business Associates and make sure they are protecting your patient information



## Compliance Tools

- ✓ HIPAA regulations are complex and confusing, our tools make complying easy!
- ✓ Track access to servers/systems with patient information
- ✓ Track CD/DVD/USB drives with patient information
- ✓ Track system activity reviews
- ✓ Termination procedure templates
- ✓ Notice of Patient Privacy (NPP) templates
- ✓ Emergency operations procedure templates
- ✓ HIPAA Technology Suite
- ✓ Many more tools and templates



## Outstanding Customer Support

- ✓ Truly outstanding customer support
- ✓ Step by step guidance – *we are with you through the whole process!*
- ✓ Ongoing guidance and advice
- ✓ Access to HIPAA experts
- ✓ Our goal is to help you with HIPAA compliance and protect patient information!



## Covered Entities and Business Associates

- ✓ Service For HIPAA Covered Entities (CE) and Business Associates (BA)
- ✓ Specialized CE and BA Risk Assessment Process
- ✓ Specialized CE and BA Policies and Procedures
- ✓ Specialized CE and BA Security Training



## Reference Library

- ✓ If you need information or have a question, we have the answer!
- ✓ Access to articles, links and HIPAA related reference material
- ✓ Curated articles on HIPAA topics
- ✓ HIPAA whitepapers and guides
- ✓ HIPAA videos on how to protect patient information

# What Is HIPAA?

## How Do You Report HIPAA Violations?

To report a HIPAA violation, you email or call the Office of Civil Rights. From their website: You may file a complaint for yourself, your organization, or for someone else. If you need help filing a civil rights, conscience and religious freedom, or health information privacy complaint, please email OCR at [OCRMail@hhs.gov](mailto:OCRMail@hhs.gov) or call 1-800-368-1019. Also, there is a portal you can use. [https://ocrportal.hhs.gov/ocr/cp/complaint\\_frontpage.jsf](https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf) But what are HIPAA violations? HIPAA Violations are any violation of any of the policies or Rules described in the legal acts of HIPAA and HITECH. They could be related to breaches of confidentiality, breaches of integrity, breaches of privacy, breaches of security, lack of availability of electronic health records, compromise of protected health information, and so much more. Remember this is a lion's den. A gray one. You're under a spider's web. If under the web lies a spider or maybe an Artificial Intelligence bot, HIPAA is a huge centipede sitting on top of it. It's all quite a mess. You really do need help with all of this.

## What are HIPAA Forms?

Policies and Procedures need to be in place, and all staff need to be familiar with them. There is a Sanction Policy, a BYOD policy, there are consent forms, and more. You shouldn't do these yourself. We worked with a HIPAA Attorney to create forms that we can customize for our clients. Again, the laws are loose and vague. Due diligence, and being able to prove it, is how you avoid hefty fines and major damage to your business continuity.



# What Is HIPAA?

## Summary of the HIPAA Security Rule from HHS.ORG:

This is a summary of key elements of the Security Rule including who is covered, what information is protected, and what safeguards must be in place to ensure appropriate protection of electronic protected health information. Because it is an overview of the Security Rule, it does not address every detail of each provision. (YIKES!)

## Introduction to HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA [Privacy Rule](#) and the HIPAA [Security Rule](#). The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called “covered entities” must put in place to secure individuals’ “electronic protected health information” (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in

# What Is HIPAA?

the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks.

(It's also strengthening the role of artificial intelligence... HIPAA is a paperwork dump on top of it!)

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

# What Is HIPAA?

## 10 HIPAA Security Tips

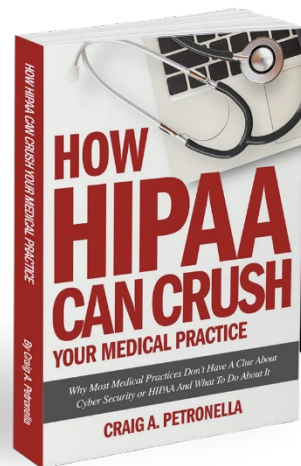
1. Have you ever had a HIPAA security risk assessment done?
2. Have you ever had a penetration test (Pen Test) done?
3. Are you using SSL website encryption, email encryption, hard disk encryption AND keystroke encryption?
4. Are you using a security solution that stops all persistent malware and ransomware threats from being able to write to the hard disk drive?
5. Are you aware of all of the important policies and procedures you need to have in place? Do you have all of these policies and procedures: Security Management Policy, Security Officer Policy, Workforce Security, Information Access Management, Security Awareness, Incident Response, Contingency Planning, Evaluation, Business Associate Contracts, Facility Access Controls, Workstations Use, Workstation Security, Physical Safeguards Device Media, Access Control, Audit Controls Policy, Integrity Policy, Person or Entity Authentication, Transimission Security Policy?
6. Do you have a BAA in place with all of your vendors? Make sure you have a business associate agreement or BAA in place with all of your vendors. I can't stress this enough. If you have just one vendor that you missed, it could cost your practice huge fines. A local medical practice just got hit with \$750,000 in fines for not having a BAA in place with a third-party x-ray company.
7. Do you have privacy screens on all of your computers, laptops and devices?

# What Is HIPAA?

8. Do you lock up any physical files that contain Patient Health Information (PHI)?
9. Does your computer screen timeout after 3 minutes or less with a password prompt?
10. Do you have the passcode and encryption features on all mobile devices, tablets, iPhones, droid devices, etc. enabled?

## A Glimpse of Light

### How HIPAA Can Crush Your Medical Practice Book



Now Available on  
Amazon by  
Craig Petronella -  
One of Amazon's  
bestselling authors

Craig Petronella  
HIPAA & Cybersecurity Expert

As we mentioned, CEO Craig Petronella is the Amazon Bestselling Author of “How HIPAA Can Crush Your Medical Practice.” The book is available on [Amazon](#); let’s take a sneak peek inside to get an overview of content:

**Section 1**.....Introduction: HIPAA Can Hurt you (AND IT WILL)

**Chapter 1**.....Are you in the HIPAA Crosshairs? Chances are, yes you



# What Is HIPAA?

are. If you are human, operating a medical practice, and not a HIPAA law expert. They have assessed fines in EXCESS of \$2 million dollars. THERE IS NO TIME TO WASTE. IT'S TIME TO WAKE UP AND COME TO THE LIGHT.

**Chapter 2**.....What does it take to comply with HIPAA? Just short of your firstborn child, really.

**Chapter 3**.....Why is failure to comply so serious? Audits are picking up- the OCR has formally announced this. IF YOU ARE GOING TO SAVE YOURSELF, YOU MUST DO IT NOW.

**Section II**.....Introduction: HIPAA Violations Can Occur Against Your Will (NOT GOOD!)

**Chapter 4**.....How do breaches happen? Ah, let us count the ways!!

**Chapter 5**.....What cyber threats do you face? All of the above! Malware, ransomware, zero-day threats.

**Chapter 6**.....Why must security maintenance be active and ongoing? Have you ever painted a constantly changing landscape?

**Section III**.....Introduction: Your Data Can Be Kidnapped (DEFINE DATA! One is just a DATUM!)

**Chapter 7**.....What Exactly is Ransomware? We won't say that it seems to be what is taking one U.S. city hostage at a time, but some would! This is a REAL threat.

**Chapter 8**.....How would ransomware ruin my day? Again, let us count the ways! Just ask the City of Baltimore!

# What Is HIPAA?

**Chapter 9**.....How can I prevent a ransomware attack? Our 22 layers of woven security solutions are the anti-threat. It's the only way we know of to break free of hostage threats!

**Section IV**.....Introduction: You can protect yourself. Did we mention our 22 layers of (mostly patented) security technologies?

**Chapter 10**.....What preventative measures can you take?

**Chapter 11**.....Why is having a quality IT provider so important? It's hard to believe that in 2019, anyone would still ask this question! World War III is on the World Wide Web, and you are being summoned...whether you like it or not!

**Chapter 12**.....How can you choose the best IT provider for you? Well, you're on our page- so you're off to a good start. In the age of information, Wisdom is the key.


**Four Pillars of IT Success Analysis**

**Actual Disasters the Four Pillars could (or did) prevent**

**Appendix**

# What Is HIPAA?

## Artificial Intelligence



It is symbolic that we end with artificial intelligence or AI. Wouldn't wisdom count as artificial intelligence? You aren't born with it. You live, and learn. You acquire wisdom. That's our Ace Card. We leverage advanced artificial intelligence in almost every part of our business model. AI gives us super powers and allows us to analyze mass amounts of information; security logs, emails, etc. looking for patterns so we can sift and sort faster. We let AI do our heavy lifting so that when security issues and patterns are found, our engineers can respond fast. We have acquired much wisdom, and we are now a force to reckon with! Artificial intelligence is leveling the playing field. Hospitals, doctors, surgeons and teams of medical professionals leverage AI technology to help perform assessments on the health of their patients. Artificial intelligence, machine learning and deep learning software can arm medical professionals with powerful tools to scan volumes of data in seconds, screening for diseases such as cancer. New technology such as Health Passport technology that leverages Blockchain technology will give patients back the control over their medical records. At the touch of a button, patients can be in full control of who sees their electronic health records, for what reason, and for how long. Don't fear AI. It will make us all super-humans, and we can be victors even as we slump around in the gray area. Machines are being trained to screen blood for diseases across a mind-blowing number of samples. Artificial Intelligence is Wisdom, and it will decide the winner of World War III. You can't use artificial intelligence safely without the proper cybersecurity controls in place. You can't be HIPAA compliant without the proper cybersecurity controls in place. Do you know of anyone else who offers our custom 22 layered approach? We don't. And we've searched. It seems that we are charged with the quest of saving the world from the gray area of HIPAA. Let WISDOM be your guide.

# Petronella – 4 Pillars Risk Assessment

## Why Should You Conduct a Risk Assessment?

Most of the business professionals we work with tell us they don't have time to really assess the risks present in their IT systems and personnel. They don't have time to assess...

- Uptime
- Security
- Applications Issues
- Collaboration Constraints

However, an in-depth analysis of the “Four Pillars” can often uncover factors that will save you at least \$100,000. What we find can help you avoid penalties, increase efficiency, minimize risk of system failure, and avoid costly downtime.

We have created videos that present a “deeper dive” into each of these Four Pillars if you'd like to learn more...

- Security Awareness Training
- Security and Compliance
- Penetration Testing
- Managed IT Security Services



# Petronella – 4 Pillars Risk Assessment

## Four Pillars Assessment Can Solve the 3 Most Common Problems IT Departments Face...

**Problem #1: Lack of Response.** When your network goes down or is experiencing a problem, it brings your entire firm to a screeching halt. With the fast pace of business today, you can't afford to wait. Our assessment will identify potential 'response issues' and outline a plan for solving them.

**Problem #2: Poor Communication and Service.** Significant risks and losses can be mitigated with proper communication procedures. Many business owners are unsatisfied with the ad hoc and unprofessional communication procedures as they relate to their IT systems. Our assessment will uncover communication challenges and map a process for streamlining communication.

**Problem #3: Recurrence of Common Problems.** Many business owners tell us that there is always something that needs to be fixed. Once one problem is solved, two more arise. This happens when your IT strategy is reactive rather than proactive. Our assessment will identify reactive issues that are costing you money and outline a proactive plan for identifying and preventing potential problems BEFORE they arise.

# Petronella – 4 Pillars Risk Assessment

## What Improvements Can You Expect?

Our metrics show, small businesses can expect...

- 25-200% increase in productivity
- 27% reduction in downtime and lost hours

...while larger businesses can often double these results.

## What Is Involved?

First, we review your strategy, computers, and servers.

We analyze your...

- MTBF (or mean time between failure).
- Data backup strategy
- Disaster recovery strategy
- Overall security plan
- Wiring and power connections
- Hardware, software, and cabling

Then we use this data to determine your five to ten AOHOs – Areas of Highest Opportunity.

These are your areas of “lowest hanging fruit.” Areas that, if they are addressed promptly, can return the largest savings in time and money.

# Petronella – 4 Pillars Risk Assessment

Here are some of the most common AOHOs we uncover with our assessment...

**1. Neglected computers, neglected servers** – software updates come out every week and many small businesses fail to install them on all machines. This can significantly shorten your MTBF and reduce your system security.

Systems that are not maintained regularly overheat and crash .If you're not on top of the hard drive it will fill up and run out. Same thing with a server.

**2. Data backup & disaster recovery issues** – most companies do not have an adequate backup and recovery strategy. Our assessment will show how to update your procedures to avoid massive data loss.

**3. Security challenges** – The most common issues we uncover are inadequate firewall protection, weak virus prevention, poor or no security update strategy, and little to no network monitoring. We'll outline a full security strategy to lockdown your systems and data.

**4. Wiring problems** – Incorrect wiring can crash a network. We find the issues and show you how to fix them quickly.

**5. Improper power protection.** Improper power protection can lead to data loss and corruption. We look at [9 different possible power protection problems](#) that can drive your system to failure.

# Petronella – 4 Pillars Risk Assessment

**6. Potential cloud service opportunities** – We routinely find opportunities that save our clients 50% or more on IT services. Most 10-plus-employee companies can save at minimum \$100,000.00 in just 5 years.

## Plus, we will...

- » identify any IT warning signs that currently exist in your IT environment
- » map out a solution to address those warning signs
- » provide you with a “battle plan” for an IT solution that will assist in your company’s business goals and catch any problems before they become disasters
- » Diagnose any ongoing problems or concerns you have with the computers on your network.
- » Scan for hidden viruses, spyware and loopholes in your network security that could allow hackers and other cybercriminals to access your confidential information.
- » Check your system backups to make sure they are not corrupted and can be recovered in case of an emergency.
- » Review your network configuration and peripheral devices to ensure that you are getting the maximum performance and speed from your machines.
- » Review your server file logs to look for looming problems or conflicts that can cause unexpected downtime.
- » Check that all security updates and patches are in place.



# Petronella – 4 Pillars Risk Assessment

## Our Goal: Simplify Your IT Strategy

We determine where you should focus your resources FIRST to add \$100,000 to your bottom line.

We compare your Four Pillars to industry benchmarks so you can see how your company ranks against competitors in your industry.



# Monthly Service Introduction

## This is a monthly turn-key service

Final Pricing is individualized and varies. Please call 877-468-2721 for details.

## Our service gets a practice compliant with HIPAA. Guaranteed.

There's a 100% satisfaction guarantee. It typically takes 4-6 months to get a practice compliant depending on complexities and the number of business associates involved. If at any time, a practice does not feel like they are getting the value provided, they can terminate the agreement and will only pay for what they've used. NOTE: PTG typically grants a license for the Security controls that are rented as part of this agreement and the HIPAA policies and procedures. The two are married together to get your practice compliant. If you terminate the agreement, your practice may no longer be HIPAA compliant and you will need to re-start the entire process with another provider.

# Month 1: Regulatory Compliance

PTG works with our clients to get them in compliance, whether it be HIPAA, NIST or ISO standards. We develop policies and procedures, training materials, and compliance infrastructure to ensure that your organization stays in compliance.

**Are you in the HIPAA Crosshairs? If you're like most PT practices, chances are you are.**

Over the next 12 months, join private, encrypted and confidential Zoom sessions with Craig Petronella, a HIPAA compliance and Cybersecurity expert who will act as your Fractional Chief Information Security and Compliance Officer:

## **Fractional Chief Information Security & Compliance Officer (CISCO)**

Senior-level executive responsible for developing and implementing information security and compliance programs. This includes attested policies, published procedures and technical controls that will protect the following from all internal and external threats: confidentiality of all stakeholders (customers, patients, employees, investors, etc.), integrity of all systems, data, and end-point devices, and availability of information communications systems.”

# Month 1: Regulatory Compliance

**Month 1:** Discuss the current state of your medical practice. Craig will walk you through a mini assessment process to help you to:

- Review what you have in place now
- Define all of the work to be done across your People, Process and Technology
- Discuss the policies and procedures that apply to your practice.
- Create a customized game plan for your practice to become HIPAA compliant; broken down into easily digestible monthly installments. Guaranteeing your practice will be compliant on or before month 12
- Discuss PTG Professional Services

**Threat and Incident Response:** Remote analysis of suspicious or malicious activities, defensive response, hardening, and documentation

**Ask Craig Anything:** IT coaching and technology advisory about IT, cybersafety or technology

**Helpdesk Support:** Live phone/remote technical support of hardware/software issues via secure remote mirroring of end-user computers and mobile devices.



# Month 2:

## What Does it Take to Comply With HIPAA?

In month 1 we discussed the mini assessment process and came up with a game plan.

In month 2, we start executing the plan.

- Discuss various HIPAA compliant security controls
- Discuss the role and responsibilities of a HIPAA privacy officer
- Discuss in-house vs outsourcing the role of a HIPAA Chief Information Security and Compliance Officer (CISCO)
- Assign one of your employees as your organization's HIPAA Chief Information Security and Compliance Officer (CISCO) and have them sign off on the responsibilities as defined in the position agreement

# Month 3: Jobs to Be Done

- Review, discuss and outline all of the jobs to be done and decide who will do the work
- Discuss pros and cons of doing the work in-house vs. outsourcing
- Review remediation options and costs of anything found in the mini assessment
- Discuss common cyber threats such as Ransomware, malware and zero-day threats
- Discuss secure, turn-key HIPAA compliant hosting vs. on-premise solutions

## Secure Hosting:

**PTG WorkSpaces:** Secure hosted desktop workspace

**PTG Unhackable Server Encryption:** Patented digital prophylaxis for servers

**PTG Unhackable Maintenance:** Proactive daily updates to operating systems, browsers and third-party applications

**PTG Upstream Bandwidth:** from PTG Cloud to your office. Up to 100 GB per month total bandwidth

# Month 3: Jobs to Be Done

**Microsoft Windows Licenses:** for server-side hosting

**Vmware Virtualization:** for hyper-visor layer

**PTG Business Continuity Level I:** Full backup on all hosted / cloud data within secure Raleigh data center

**PTG Cloud file share:** (super secure Dropbox like service)

**PTG Domain Controller for User Active Directory:** configured to your practice

**PTG Dynamic Resource Allocation:** Dynamic expansion of RAM and CPU threads to ensure quality user experience

**PTG Endpoint Antivirus:** Real-time attack monitoring and defense of end-user computers from server-side prophylaxis (compliments existing anti-virus packages)

**PTG Firewall:** router & access logging and monitoring, required for HIPAA compliance

**PTG Remote-access VPN:** encryption of all user access from public WiFi and open networks

# Month 3: Jobs to Be Done

**PTG Technical Support of Secure Hosting:** 24x7x365 via phone, email, or ticket for hosting related issues

*Does not cover IT user support inhouse or personal-use computers, laptops, smartphones or wearables*

**PTG Multi-factor User Authentication:** configured with user training guide and HIPAA Policies

**Microsoft Office 365 E3:** HIPAA compliant, includes BAA from Microsoft

**PTG Unhackable Website:** Patented digital prophylaxis for your Website, blogs and related media. Transport Layer Security

Website content backup

Visitor Geo-blocking

Distributed Denial of Service (DDOS) protection



# Month 4: Security Controls

- Review security controls and associated cost options that apply to your practice
- Discuss approved and recommended vendor options for on-premise security controls vs hosted solutions
- Discuss PTG Managed Services

**PTG Encrypted DNS:** Encrypted Domain Name Service (eDNS) - Encrypts website traffic, automatically blocks malicious websites

**PTG Encrypted Password Management:** for all devices with monitoring, multifactor authentication, hardware token, 100+ policies and procedures

*NOTE: This includes the use of a hardware token, eliminating the vulnerability associated with remembering and inputting passwords*

**PTG Endpoints Forcefield:** Security controls configured against HIPAA Policies for computers, smart phones, phone systems

*NOTE: This entails a weekly protocol for validating that your HIPAA-mandated controls are functioning; includes audit trail and the ability to provide a report of compliance*

**PTG Unhackable Email Encryption:** Patented digital prophylaxis for all email exchanges

**PTG Threat Landscape Management:** Proactive monitoring of threat landscape and direct surveillance of malicious penetration attempts, logging and maintenance, across your entire IT infrastructure

# Month 4: Security Controls

**PTG Website Forcefield:** Reconfigure WordPress (or other CMS), install firewall, malware scanner, IP address blocking

**PTG Unhackable Maintenance:** Proactive daily updates to operating systems, browsers and third-party applications

**PTG Unhackable System Encryption:** Patented digital prophylaxis for desktop, laptop, and mobile devices

**PTG Unhackable MS Office 365:** Patented digital prophylaxis. Maximum security hardening: Notifications for any unusual behavior (changes to mailboxes, forwarding, rules, logins, etc.) as well as implementation and monitoring of the two-factor user authentication

**PTG Office 365 Email 100% Uptime:** Patented digital prophylaxis that guarantees that your users will have send/receive email capabilities, Addresses downtime of Office 365

**PTG Unhackable Endpoint 100GB Backups:** Daily virus-free backups of end-user computers (phones and tablets not covered)

**PTG Unhackable Cloud Storage:** Secure Replacement for Microsoft OneDrive: Enterprise file sync and sharing. Improved levels permissions, files control, reporting, auditing. Remote wipes of stolen or lost computers or smartphones

**PTG HIPAA Compliant Phone Service:** with Polycom VVX 350 phones, signed BAA and monitoring as required by HIPAA

# Month 4: Security Controls

**PTG Unhackable Virtual Private Network:** Patented digital prophylaxis for remote access from any public network. Secure Use of Public WiFi. Tunneling: users may use any WiFi network with assured privacy. Encrypted access: Defeats WiFi network sniffing and capture of user credentials

**“PTG CloudUTM:** Enterprise Managed Firewall with the ability to support failover

## SUMMARY

- New faster/more reliable firewall equipment with lifetime warranty. If equipment fails, we replace it FREE
- Segmentation
- More reliable and with multiple, secure, network segments
- State of the art security and filtering
- Granular control of the network by using dedicated equipment paired with our CloudUTM with reduced latency
- Block categories of web traffic and run detailed reports

# Month 5: Important Policies and Procedures

- Review and discuss basic HIPAA policies and procedures
- Begin customizing the HIPAA policies and procedures
- Train staff on how to store the basic HIPAA policies and procedures in the secure, encrypted portal

HIPAA Security Policy #1 - Security Management Policy

HIPAA Security Policy #2 - Security Officer Policy

HIPAA Security Policy #3 - Workforce Security

HIPAA Security Policy #4 - Information Access Management

HIPAA Security Policy #5 - Security Awareness

HIPAA Security Policy #6 - Incident Response

HIPAA Security Policy #7 - Contingency Planning

HIPAA Security Policy #8 - Evaluation

HIPAA Security Policy #9 - Business Associate Contracts

HIPAA Security Policy #10 - Facility Access Controls

HIPAA Security Policy #11 - Workstations Use

HIPAA Security Policy #12 - Workstation Security

HIPAA Security Policy #13 - Physical Safeguards Device Media

HIPAA Security Policy #14 - Access Control

HIPAA Security Policy #15 - Audit Controls Policy

HIPAA Security Policy #16 - Integrity Policy

HIPAA Security Policy #17 - Person or Entity Authentication

HIPAA Security Policy #18 - Transmission Security Policy



# Month 6: HIPAA Security Awareness Training

- Discuss common breach types across all aspects of People, Process and Technology
- Setup HIPAA Security Awareness Training for your staff
- Review and introduce staff to the training portal
- Set a goal of when your staff will complete the training
- Schedule testing for your staff to receive a certificate of compliance

# Month 7: HIPAA Training Continued...

- Train and Quiz staff on common HIPAA infractions
- Discuss the importance of compliance and the ramifications of non-compliance
- Discuss potential infractions and how to avoid

# Month 8: Risk Assessment Overview

- Discuss the risk assessment process
- Re-assess remediation steps in prior months
- Define what work is left to be done and decide if the timing is right to begin the annual security risk assessment

Our Consultants work to ensure that your organization is fully informed regarding its risks. We perform comprehensive qualitative assessments that will give your organization a clear picture of its risk landscape. We also help prioritize risk mitigation, implement mitigation measures, and manage your organization's threats, vulnerabilities and costs related to information security.

# Month 9: Compliance Services

- Begin Risk Assessment
- Organize all organization assets
- Begin risk assessment process
- Schedule HIPAA audit

## Discuss PTG Compliance Services:

**PTG HIPAA Security Risk Assessment:** Annual assessment of practice as required by HIPAA

**PTG/MEG HIPAA Bootcamp:** 12 Self-directed online training videos and activities with PTG Quizzes and worksheets graded for each module

**PTG HIPAA Policy Kit:** Boiler plate policies and procedures customized to your practice per HIPAA requirements

**PTG HIPAA Documentation Service:** Customization of Policies and Procedures that comply with HIPAA requirements

**PTG Website Policy Kit:** Boiler plate policies and procedures customized to your practice per HIPAA requirements

**Cyber Insurance for HIPAA Breach and Fine Expenses:**  
\$250,000 policy



# Month 9: Compliance Services

**PTG Security Awareness User Training and Certification:** Self-directed online training videos and activities with PTG Certificate of Compliance for each employee

**PTG User Training and Certification for HIPAA:** Self-directed online training videos and activities with PTG Certificate of Compliance for each employee

**PTG Business Associate Agreement (BAA) Service:** Customization of your BA agreements (for legal attestation)

**PTG Simulated Phishing Campaigns:** A phishing test is where deceptive emails, similar to malicious emails, are sent by an organization to their own staff to gauge their response to phishing and similar email attacks

**PTG Employee Vulnerability Assessment:** Find out which employee(s) are at high risk to potentially cause a data breach!

**PTG Unhackable Newsletter:** Regular updates about the current IT security threats, cybercrime tactics, cyberheist schemes, social engineering scams and ransomware attacks. Includes hints and tips to help you block hackers that could cause a HIPAA breach

**PTG Dark Web Monitoring:** Also known as cyber monitoring, is an identity theft prevention product that enables you to monitor your identity information on the dark web, and receive notifications if your information is found online

# Month 9: Compliance Services

## PTG Weekly Micro-Training Video & Quiz

**PTG Situation Awareness & Reporting:** Monthly review of Proactive Cybersafety activities and counter measures

**PTG Breach Reporting:** In the event of the actual or suspected breach of PHI/PII, PTG Breach Reporting notifies Federal and State regulatory authorities and consumers as mandated. Your call to PTG about a potential privacy breach will initiate an immediate evaluation of your incident; PTG will determine whether or not to notify authorities and consumers. PTG will file the necessary breach reports on your behalf, leaving it to you notify your patients and affiliates with inputs and talking points from PTG

**PTG Incidence Reports for OCR:** Preparation of report of findings and remediations (where applicable) for submission to Office for Civil Rights of US Dept of HHS

# Month 10: Remediation

- Discuss issues found
- Discuss remediation options
- Discuss the various types of IT support available to you and cost options
- Discuss the importance of ongoing monitoring and maintenance
- Begin Remediation

# Month 11: Remediation Continued

- Finalize all open remediation issues
- Schedule final interview with HIPAA underwriting team
- Discuss included PTG Breach Response Services

If your organization's security of PHI has been breached, we promptly will:

- Advise on reporting responsibilities
- Assist with breach mitigation
- Conduct Breach Risk Assessment in accordance with regulatory requirements
- Develop and implement Plan of Correction



# Month 12: HIPAA Compliant and Peace of Mind

- Receive HIPAA certificate (good for 1 year) of compliance with customized policies and procedures customized against security controls as defined above
- Discuss ongoing work to be done, security maintenance, monitoring and controls to remain in-compliance with HIPAA
- Discuss ENFORCEMENT ACTIONS AND LITIGATION SUPPORT. If your organization is facing enforcement actions or litigation, we will work with you and your legal counsel as an expert witness
- Discuss DATA PRIVACY & SECURITY

Our data privacy and security practice ensures that your information is protected at all times. PTG consultants provide the industry knowledge and support to keep your organization and its assets safe and reduce vulnerabilities

*Great Results, Expert, Creative. Craig is a motivated, detail-oriented individual who strives to provide the highest quality IT support and equipment for his clients. He responds quickly and efficiently when issues arise and we have had much success with his management of our entire IT network. He keeps our busy family practice EMR and server going at all times, as we are open 7 days a week. We would recommend his services highly.*

Healthcare practice in Raleigh-Durham, NC

---

*I would recommend him to any client who is looking for any IT help for their organization. I have worked with Craig with implementation of EMR (Electronic Medical Records) in the Durham area. He is extremely professional and very knowledgeable with the current technologies. He ensured that we never had any issues with the IT infrastructure at the practice and that was one of the primary reasons that the implementation went smoothly. He scored high points with his client and us with his professionalism and knowledge and I would recommend him to any client who is looking for any IT help for their organization.*

Jaimin Anandjiwala  
Director of Enterprise Business Division eClinicalWorks EMR

---

*Petronella's work has been a major factor in our business success, helping it to become one of the most secured network of its kind on the Internet. I confirm that I have dealt with Craig over past year, during which time he has provided my business with excellent support in the areas of network consultation, help-desk support, security monitoring and server monitoring. His work has been a major factor in our business success, helping it to become one of the most secured network of its kind on the Internet. I can confidently recommend Craig's company and its services as a solid and reliable supplier and as experts in their field. At all times I have found Craig to be dependable, reliable, hard-working, conscientious, honest, peace-loving, courteous, and as helpful as possible.*

Financial Services Firm in Raleigh, NC

