



### Compliance Law Changes:

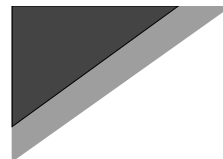
**HIPAA, OIG, CURES & No Surprises Act** - Why they are after you? How they catch you? What they do to you?  
How to avoid being a statistic!

**Dr. Ty Talcott, CHPSE**

C: 469.371.8804 / PH: 214.437.7559

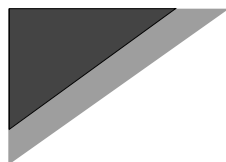
[Ty.talcott@gmail.com](mailto:Ty.talcott@gmail.com) / [Info.hipaa@gmail.com](mailto:Info.hipaa@gmail.com)

1



A Little about me.

2



Foxworth video

3

### Who Is Dr Ty The Compliance Guy?

- First Chiropractor to hit \$1 Million
- Became consultant for Chiropractors after retiring from practice
- 48 associations and 5 colleges
- Leader in compliance for chiropractors

4

## My Story



- I wasn't always the "compliance guy" - I used to never know anything about HIPAA...
- Now I've helped over 7,000 chiropractors...

Hands-Off HIPAA Compliance

5



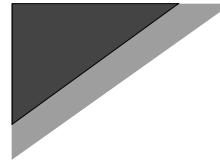
6



## Ski Lift Acrobatics

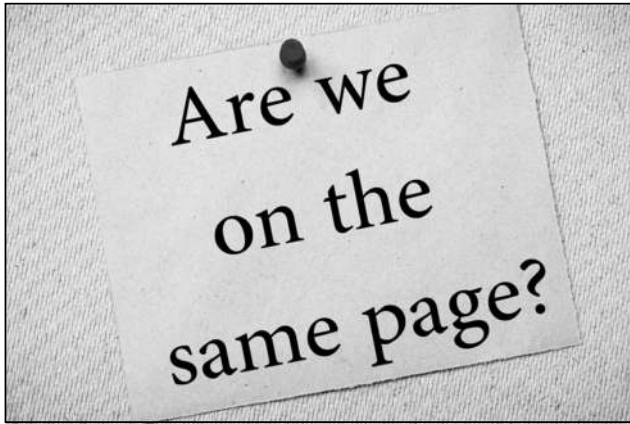


7



How do they catch people

8



## Civil Rights Director



"The idea after that is to have a permanent program, part of which **will need to be funded by the proceeds of enforcement...**  
I saw these articles out there that said 'More audits are coming' and 'Are you ready for audits?' and that's a smart question because **that is really what's ahead for us.**"

- HIMSS Privacy & Security Conference (Dec 2012)

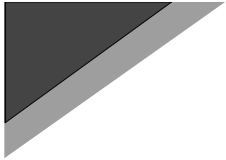
## How They Catch You!



## "The Convertible"

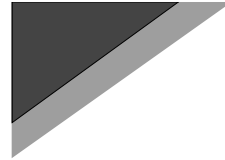


# HUMAN ERROR



\$289,000  
 Will you receive that level of  
 fine?

13



1 – 2 – 3

14

TV Expose

Be Honest...

How many of you thought  
 you just needed to have a  
 HIPAA program set up,  
 put it on your shelf and  
 train on it once per year?



Hands-Off HIPAA Compliance

15

16

## Two Components To HIPAA



1. Must Have A HIPAA Program INSTALLED
2. Your "Installed" Program Must Be ACTIVE & DYNAMIC

Hands-Off HIPAA Compliance

17

## Why Active & Dynamic?

- The whole purpose of compliance is to protect your patients' health information.
- The same measures we used 10 years ago aren't effective, so it must be active and dynamic to meet the current needs of the day.

Hands-Off HIPAA Compliance

18

## What Does Active & Dynamic Mean?



Hands-Off HIPAA Compliance

19

## How Do You Do That?

- Step 1 - Keep To Your Audit Schedule
- Step 2 - Issue Security Reminders
- Step 3 - Respond To Changes

Hands-Off HIPAA Compliance

20



Hands-Off HIPAA Compliance

21



## Cyber-security / Ransom Ware

Quote from the fall 2019 Cyber-Security Symposium:  
“A single Cyber attack has the potential to shut down care facilities, erase important patients’ information and health histories forever and put patients health and identity at risk.

This is an enterprise issue not just I.T.

22

Ledet video

23



## Success for Dr. Ledet with our help!



DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY  
Office for Civil Rights, Room 321 (Old Atlanta)  
1101 N. Independence Mall West  
Philadelphia, PA 19106-5054  
Toll-free: (1-877) 684-6461  
TDD: (215) 861-4880  
Fax: (215) 861-4882  
http://www.hhs.gov/ocr

Reference:  
Investigator:  
Contact Telephone:

February 21, 2018

Dr. Kathleen Ledet  
Ledet Family Chiropractic Center

Dear Dr. Ledet:

On July 9, 2017, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received a breach report indicating that Ledet Family Chiropractic Center was not in compliance with the Federal Standards for Privacy of Individually Identifiable Health Information and/or Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules. Specifically, the breach report indicated that Ledet Family Chiropractic Center's server was infected with ransomware.

In response to the breach, Ledet Family Chiropractic Center notified the media and affected individuals, and provided free credit monitoring to affected individuals. Ledet Family Chiropractic Center disabled the ability to remotely access the server, and required passwords to be strengthened. Ledet Family Chiropractic Center also upgraded its anti-malware software.

**We helped Dr. Ledet!** With our Hands Off HIPAA program!

All matters raised by this complaint at the time it was filed have now been resolved through the voluntary compliance actions of Ledet Family Chiropractic Center. Therefore, OCR is closing this case.

OCR's determination as stated in this letter applies only to the allegations in this complaint that

24

INITIAL DATA REQUEST

In connection with OCR's investigation into the matters raised by the breach report, we request that [REDACTED] provide the following information to OCR within fourteen (14) business days from receipt of this letter.

Please number responses to correspond with the enumerated requests. *Electronic copies are encouraged. Please no staples or double sided pages.*

1. The name, title, email address, mailing address, and telephone number of the individual(s) designated to work with OCR during the subject investigation.
2. Please provide all policies and procedures produced and implemented by [REDACTED] to address the Privacy Rule, Security Rule, and the Breach Notification Rule. For each policy and procedure, please state the date of implementation and date(s) of any revisions. Please clearly label each document provided.

25

3. Please describe how [REDACTED] assessed the number of individuals affected by the breach.
4. Please provide a copy of [REDACTED] policies and procedures for addressing security incidents pursuant to 45 CFR §164.308(a) (6) (i). Please provide the date each policy was implemented and the date(s) of any revision(s). Please provide the incident report for this particular breach.
5. Please provide a copy of [REDACTED] forensic report.

For the forensic report please state:

- a. The date the analysis was completed; and
- b. Whether [REDACTED] completed the analysis or whether it was conducted by a third party

26

6. Please provide a copy of [REDACTED] most recent risk analyses and risk management plans *within the past two years* pursuant to 45 C.F.R. §164.308(a)(1)(ii)(A) and §164.308(1)(ii)(B).

For each risk analysis produced, please state:

- c. The date analysis was completed;
- d. Whether [REDACTED] completed the analysis or whether it was conducted by a third party; and
- e. Whether the analysis was conducted enterprise-wide or compartmentalized (i.e. an analysis of a particular department or system).

If no risk analysis has been performed, please provide a written description of the

27

circumstances.

7. Please describe and provide evidence of [REDACTED] policies and procedures in place to routinely review auditing controls pursuant to 45 C.F.R. §164.312(b).
8. Please provide [REDACTED] policies and procedures for creating, changing, and safeguarding passwords. For any policies or procedures produced, please provide the date such policy was implemented and the date(s) of any revision(s).
9. Please describe and provide evidence of [REDACTED] security awareness and training program pursuant to 45 C.F.R. § 164.308(a)(5)(i), including:
  - a. how often training is conducted;
  - b. copies of training materials (ex: print outs of module training screens, power point slides, etc.); *The materials should be dated;*
  - c. how workforce training is tracked/monitored;
  - d. how training completion is enforced; and
  - e. documentation that workforce members, including managers, completed all required training in 2018 and 2019.

28

13. Please provide a written description of [REDACTED] mitigating actions taken in response to this incident pursuant to 45 C.F.R. §164.530(f)(1).
14. Please fill-in the right column of the below chart by inserting the title of the corresponding policy(s) and/or procedure(s) implemented by [REDACTED] intended to address each specific provision listed in the left-hand column. [REDACTED] may insert the same policy or procedure for multiple provisions, as long as said policy or procedure is applicable to those provisions. If a policy, procedure, or other documentation has not been produced to address a specific provision, please provide a written explanation detailing the circumstances.

29

Provision(s):	Applicable Policy and/or Procedure:
Impermissible Uses & Disclosures: 45 C.F.R. §164.502(a)	
Minimum Necessary: 45 C.F.R. § 164.514(d)(1)-(2)	
Safeguards: 45 C.F.R. §164.530(c)	
Mitigation: 45 C.F.R. §164.530(f)(1)	
Security Management Process: 45 C.F.R. §164.308(a)(1)(i)	
Risk Assessment: 45 C.F.R. §164.308(a)(1)(ii)(A)	
Risk Management 45 C.F.R. §164.308(a)(1)(ii)(B)	
Security Awareness and Training: 45 C.F.R. §164.308(a)(5)(i)	

30

Audit Control: 45 C.F.R. §164.312(b)	
Information System Activity Review: 45 C.F.R. §164.308(a)(1)(ii)(D)	
Information Access Management: 45 C.F.R. §164.308(a)(4)(i)	
Security Incident Procedures: 45 C.F.R. §164.308(a)(6)(i)	
Device and Media Controls: 45 C.F.R. § 164.310(d)(1)	
Encryption and Decryption: 45 C.F.R. § 164.310(d)(1)	
Accountability: 45 C.F.R. §164.310(d)(2)(iii)	
Password Management: 45 C.F.R. § 164.308 (a)(5)(ii)(D)	
Facility Access Controls: 45 C.F.R. §164.310(a)(1)	

31

15. For OCR's accountability purposes, and to provide context for the investigation, we are requesting that you provide us with the following information in relation to [REDACTED]:

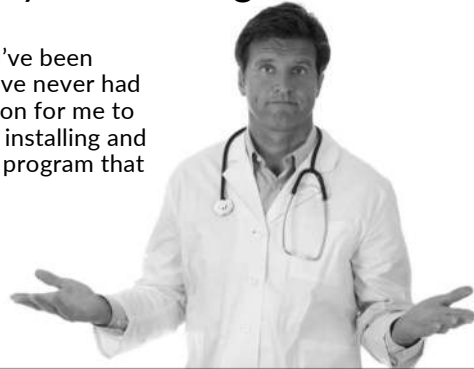
- (a) Geographic area served;
- (b) Number of facilities/locations;
- (c) Number of employees in 2018 and currently;
- (d) Number of patients served in 2018; and
- (e) Operating budget for 2018.

32



## You May Be Thinking...

"Ty, I'll never get audited. I've been doing this for years and have never had a problem. There's no reason for me to waste my time and money installing and maintaining a New HIPAA program that I'll never use."



Hands-Off HIPAA Compliance

33

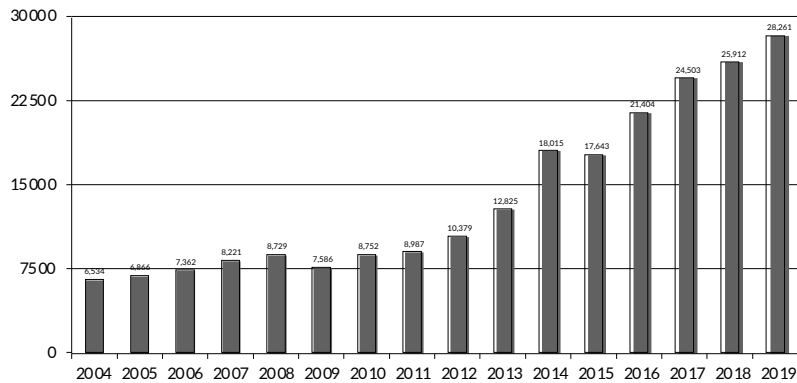
## I Used To Think That Too...

- But Now I get 2-4 calls per month of people getting investigated
- We can conservatively estimate there are around 20-40 investigations per month
- The numbers are only going up

Hands-Off HIPAA Compliance

34

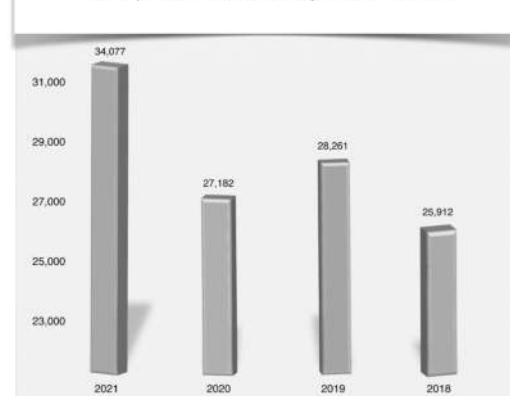
### Complaints Received by Calendar Year



Hands-Off HIPAA Compliance

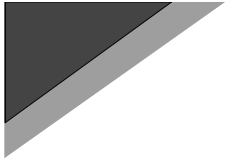
35

### Complaints Received by Calendar Year



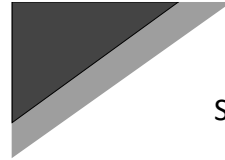
Hands-Off HIPAA Compliance

36



## OIG - Medicare

37



So, let's go back to HIPAA and look at an overview of what we have to put in place - show extreme good faith - to nearly bullet proof ourselves from fines, ransom ware and/or shutting down your business from other types of cyber attack-- before diving in depth on some of these issues. This is no longer just avoiding fines.. it is about protecting your business!

38

## What's Included In Your HIPAA Manual?

- Usually between 300-800 pages
- Customized to your specific office
- Let me give you an overview of what a HIPAA Regulatory Compliance Manual looks like

39

## HIPAA Regulatory Compliance Manual

- |   |  |
|---|--|
| 1. Compliance Officer                           | 9. Physical Plant Audit  |
| 2. Notice of Patient Privacy Policy             | 10. Risk Analysis  |
| 3. Forms  | 11. ISAR   |
| 4. Required Accounting Log                      | 12. Required Annual A-Z HIPAA Program Audit/Evaluation                         |
| 5. Corrective Action Forms                      | 13. BONUS Audits   |
| 6. Employee Confidentiality Statements          | 14. Policies and Procedures for Security Rules                                 |
| 7. Business Associate Confidentiality Contracts | 15. Required Contingency Plan with Data Recovery And Emergency Mode Operations |
| 8. Annual Required Staff In-Service Training    |  |

40

## Policies & Procedures

- PRIVACY OFFICER/COMPLIANCE OFFICER
- PRODUCTION OF DOCUMENTS AND DATA
- RETENTION OF DOCUMENTS AND DATA
- SANCTION POLICY
- CONFIDENTIALITY AGREEMENTS AND B.A. CONTRACTS
- SCOPE OF PROTECTION UNDER THE SECURITY RULES
- APPLICABLE STATUTES / REGULATIONS
- TEAM MEMBER/WORKFORCE POLICIES
- PROHIBITED ACTIVITIES
- SECURITY MANAGEMENT PROCESS- RISK ANALYSIS
- EMERGENCY OPERATIONS PROCEDURE
- EMERGENCY ACCESS
- BUILDING SECURITY
- ELECTRONIC COMMUNICATION
- INTERNET ACCESS
- REPORTING SOFTWARE MALFUNCTIONS
- TRANSFER OF FILES BETWEEN HOME AND WORK OR EMPLOYEE TO EMPLOYEE
- INTERNET CONSIDERATIONS
- DE-IDENTIFICATION / RE-IDENTIFICATION OF PERSONAL HEALTH INFORMATION (PHI)
- USER LOGON AND IDS
- ACCESS CONTROL
- DIAL-IN CONNECTIONS
- MALICIOUS CODE
- ENCRYPTION
- TELECOMMUTING
- SPECIFIC PROTOCOLS AND DEVICES
- RETENTION / DESTRUCTION OF MEDICAL INFORMATION
- DISPOSAL OF EXTERNAL MEDIA / HARDWARE
- MANAGING CHANGE
- AUDIT CONTROLS
- BREACH NOTIFICATION PROCEDURES
- CONFIDENTIALITY / SECURITY TEAM (CST)
- CONTINGENCY PLAN
- SECURITY AWARENESS AND TRAINING
- EMPLOYEE BACKGROUND CHECKS

Hands-Off HIPAA Compliance

41



Hands-Off HIPAA Compliance

42

## Is Your HIPAA Program Complete?

“We thought we were compliant with HIPAA regulations, and we were doing a lot of things right. That’s the good news!

But what we didn’t know about what was expected for privacy and security was overwhelming. That was the bad news!

We now know that our systems are much tighter, our policies and procedures are more complete, and that we are doing everything in our power to protect our patients’ information.”

- Kathy Hoff, Director of Community Relations

Hands-Off HIPAA Compliance

43

## You Might Also Be Thinking...

Hands-Off HIPAA Compliance

44

“Dr. Ty This Looks Like  
An Awful Lot Of Work!”

Hands-Off HIPAA Compliance

45

The Truth Is...

Hands-Off HIPAA Compliance

46

IT IS A LOT OF WORK!

Hands-Off HIPAA Compliance

47

You Might Be Feeling...

Like One Doctor Who Told Me...

“Even if I could figure out how to do the ongoing training, which is  
doubtful, it is unlikely I would actually follow through.”

Hands-Off HIPAA Compliance

48

## So What Do You Do?

- Do it yourself?
- Dredge everything up once a month...
- Find what you did last year and try to remember how it all works...
- Google search or go to a seminar to see what the new requirements are...
- Write up a security reminder every month and distribute it...
- Oh... and it has to include new cyber threats

## What If I Told You...

You Don't Have To Worry About  
ANY Of This!

Introducing...

## Hands-Off HIPAA Compliance: A Done-For-You Program

Hands-Off HIPAA Compliance

53

"Hands-Off HIPAA Compliance" is all about



- Helping you Install and Maintain your HIPAA program in as little time as possible...
- So you can focus on your practice
- So you can help and protect your patients
- So you can practice stress-free knowing you have a defensible position

Hands-Off HIPAA Compliance

54

Here's What You Get...

Hands-Off HIPAA Compliance

55

"Complete HIPAA Compliance Manual"

- We author your HIPAA compliance manual for you: Risk Analysis, ISAR, around 100 pages of policies, customized documents and forms, and much more!
- Everything you need to be compliant (usually 300–800 pages)
- We send you a questionnaire, you answer it and we put together your manual based on what your practice needs. (It's different for everyone)
- We have it in Digital Format
- Also Physical copy as well.

Hands-Off HIPAA Compliance

56

## “But Dr. Ty, I Have A HIPAA Program!”

- Do you have everything we just went over?
- Do you have and did you sign off on a risk analysis, mitigation plan and at least four ISAR's in the last year?
- Do you have and did you SIGN OFF on, about a dozen HIPAA reviews, evaluations and audits in the last year (about one per month)?
- Did you issue a security reminder to your staff last month and have one ready for this month?
- In my experience 99% of practices don't have everything they need

Hands-Off HIPAA Compliance

57

“I have to say I love Dr. Ty Talcott's MMM Program. It has made my life so much easier along with my HIPAA compliance.

I get the form(s) emailed to me every month, so I don't even have to worry about it. I just follow the directions, complete the form and file in my HIPAA manual.

Well worth the monthly fee! Thank you Dr. Ty!”



Dr. Kristine Springer

Hands-Off HIPAA Compliance

59

## **SEVEN (7) FREE GIFTS** **included with the purchase of every HIPAA program!**

**OIG COMPLIANCE PROGRAM FOR FREE**  
(OIG Program DIY Manual; a \$399 value)

**TWO (2) FREE MONTHS OF MMM**  
(Mandatory Monthly Maintenance program; a \$58 value)

**REQUIRED ANNUAL STAFF TRAINING FOR FREE**  
(must be done within 45 days of each new hire; a \$185 value)

**ALERT LIST – FREE NEWSLETTER**  
(we continually provide law and enforcement changes plus updated compliance forms)

**OSHA – FREE DIY MANUAL**  
(includes training for a standard office; a \$159 value)

**NO SURPRISES ACT - FREE**  
(Templates, Instructions and GFE: *Good Faith Estimate*; a \$225 value)

**ONC – FREE Information Blocking Law**  
(Policies, Templates, and Instructions; a \$89 value)

58

## We've Got Your Back Guarantee

- If you are ever audited... We've got your back
- We'll fight with you. Tell you what to do, what not to do and help you navigate the whole thing

Get Started Now [DrTyTheComplianceGuy.com/go](http://DrTyTheComplianceGuy.com/go)

Hands-Off HIPAA Compliance

60

**What You're Going To Get:**

- Complete HIPAA Compliance Manual..... (\$20,000 Value)
- Mandatory Monthly Maintenance Program..... (\$2,000 Value)
- Implementation Hand Hold Checklist..... (\$997 Value)
- DIY HIPAA Program Workbook..... (\$547 Value)
- HIPAA Compliance Customizer..... (\$10,000 Value)
- BONUS: OIG Manual..... (\$400 Value)

Total Value: \$33,944

Get Started Now For Just

**\$299/mo  
for 6 months**



**Let's Do This!**

Get Started Now [DrTyTheComplianceGuy.com/go](http://DrTyTheComplianceGuy.com/go)

Hands-Off HIPAA Compliance

61



62

**Special Offer DIY Kit**

- Retail Price of ~~\$549.00~~
- Discounted Webinar Price of **\$397.00**
- **7 Free Gifts** ( \$1200+ Retail Value!)

Call **214-437-7559** or

Email: [Ty.talcott@gmail.com](mailto:Ty.talcott@gmail.com) /  
[DrTyCompliance@gmail.com](mailto:DrTyCompliance@gmail.com)

**What You're Going To Get:**

- Complete HIPAA Compliance Manual..... (\$10,000 Value)
- Mandatory Monthly Maintenance Program..... (\$2,000 Value)
- Implementation Hand Hold Checklist..... (\$997 Value)
- DIY HIPAA Program Workbook..... (\$547 Value)
- HIPAA Compliance Customizer..... (\$4,000 Value)
- BONUS: OIG Manual..... (\$400 Value)
- Fast Action BONUS: Perfect Practice Solutions... (\$1,000 Value)

Total Value: \$18,944

Get Started Now For Just

**\$299/mo  
OR  
\$99/mo**

PH: 214-437-7559 or  
[Ty.Talcott@gmail.com](mailto:Ty.Talcott@gmail.com) /  
[DrTyCompliance@gmail.com](mailto:DrTyCompliance@gmail.com)



**Let's Do This!**

Get Started Now [DrTyTheComplianceGuy.com/go](http://DrTyTheComplianceGuy.com/go)

Hands-Off HIPAA Compliance

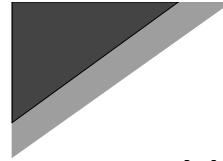
63

64



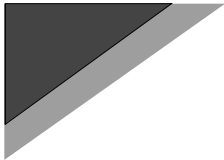


65



More likely to have a major financial impact from a government compliance fine than a malpractice suit.

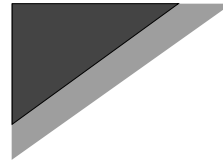
66



**New Law April 5, 2021**


Information Blocking Law  
Not HIPAA, but supersedes parts about PHI.

67




21<sup>st</sup> Century CURES ACT  
45CFR 145 and is enforced  
by ONC / Office of National Coordinator  
– under  
Health and Human Services / HHS  
and Office of Inspector General / OIG.

68



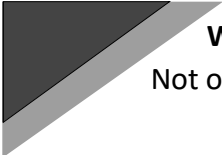
**Remember:** we are NOT attorneys and are NOT offering legal advice. These are fluid situations that will be ever changing. You are responsible to be current and stay current relative to state and federal laws that regulate your profession. We offer suggestion and assistance that can be utilized, modified or ignored. We make no representation as to the accuracy of our opinions or usefulness of our suggestions or products

69



**DIRECTLY IMPACTS CHIROPRACTORS**  
-very long, confusing law – we will take one at a time.  
**MUST provide patients electronic access to their records free (portal) and copies electronically if requested (and charge allowed rates).**

70



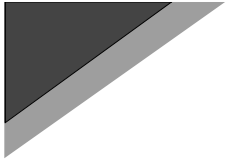
**What will be required to comply?**  
Not our main specialty, **but**, MMM module  
Or  
Audit tool.  
Mitigation plan.  
Write new policies.  
Write new procedures.  
New forms to document denials.  
Robust enforcement plan.  
Required training and proof of same.

71



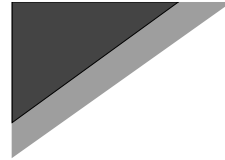
**Safe Harbor Jan 2021**

72



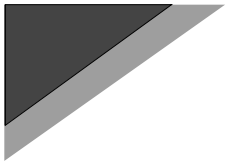
Trump Jan. 2021  
Amendment to the Hi-Tech law  
Takes 12 months...

73



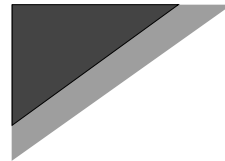
YOU HAVE TO START  
NOW!

74



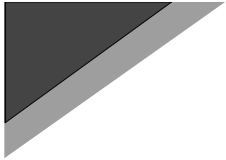
Required:  
Adopted some of Cyber security best  
practices  
Completed a risk analysis  
Reduced identifiable risks  
Implemented technical safeguards

75



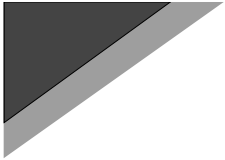
My Buddy

76



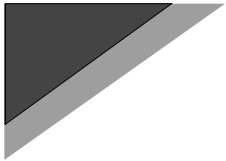
Most common HIPAA and other compliance program deficiencies that get people in trouble:

77



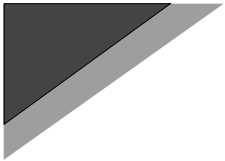
**First;**  
2021 = the year of small practice attacks and fines

78




Risk Analysis  
ISAR  
Policies  
No risk management

79




Records release - electronic and paper  
No BAA  
No NPPP

80



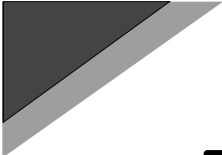
You must give a GFE, Good Faith Estimate of cost and get patient consent for fees, **if the patient is SELF-PAY OR CHOOSES TO NOT USE THEIR INSURANCE** AND this applies to new and returning patients, as of **January 1, 2022!!!!**

81



IF you don't do this and the patient complains, you can lose your fee and they can take enforcement actions against you including fines of up to \$10,000 per violation.

82



**There are no specific REQUIRED forms, However, the government has created some samples.**

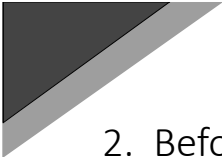
83




**Recommended processes:**

1. On Phone, before first visit, ascertain if they are self pay or have insurance and not using it. If so, be sure to give verbal notification of fees or fee range. -Have that ready in writing for them to **sign** when they arrive.

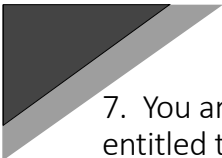
84

- 
2. Before ANY other services, with a cost rendered, explain the fees, get signature.
  3. Do a report of findings prior to treatment and verbally go over the costs- get signature.

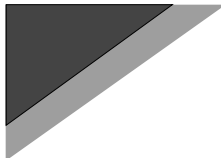
85

- 
4. Carefully monitor your care package and change it with sign off on fees.
  5. Remember, Medicare patients are paying for NON covered services out of pocket
  6. ABN for Medicare

86

- 
7. You are required to post that the patient is entitled to, can request and will be given a good faith estimate of fees if they are a cash paying patient
  8. If your care plan includes referral for other treatment (massage, PT, etc.) you must include.
  9. For new patients; You can do one estimate for reoccurring services
  10. For a patient with a new episode: treat them like a new patient

87



Dentist felt compelled to rebut a Google Review—lack of policies cost \$10k

88

- Alert list
- CHUSA
- OIG/MEDICARE webinar link
- Copy of power point notes
- Access to FREE webinars and white papers at [www.DrTytheComplianceGuy.com](http://www.DrTytheComplianceGuy.com)

89

## Risk Analysis

OCR is confused by the Senators

90

- Risk Analysis
- Date performed \_\_\_\_\_  
Participants \_\_\_\_\_
- Inventory of Assets that contain PHI, including key staff, business associates, etc.:
  - Lap Top Computer
  - On-site server
  - \_\_\_\_\_, etc.

91

- Item from inventory list:** Lap Top computer
- **Threats and vulnerabilities:**
    1. Viruses
    2. Lack of adequate policies and procedures for who uses computer - for what purposes
    3. Unknown location overnight
    4. No protocols to prevent unauthorized internet access
    5. At risk for theft while being transported
    6. Data at rest not encrypted
    7. \_\_\_\_\_ etc.

92



• **Present controls in place:**

4. There is a policy in place to limit unauthorized utilization of the internet
5. When transported in the car the computer is to always be locked in the trunk if left in the car

93



• **Gap analysis - Still needed:**

1. Anti Virus
2. Adequate Policies and Procedures need to be developed and trained to staff
3. System for 'checking out' the computer, if taken off premises, to know who has it and when it is to be returned
6. Non-encrypted data

94



• **Potential solutions:**

1. Install anti-virus, buy new
2. Install anti-virus as 'additional computer' on an existing plan
3. Download anti-virus from the internet.
4. Consider McAfee, Norton, AVG, Sophos
5. Policies could be written from scratch on each individual area needed.
6. Existing Policies could be expanded to cover areas of concern.

95

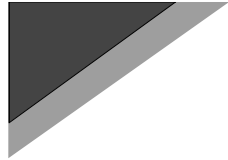


• **Mitigation of risk:**

1. Download and install Norton anti-virus
2. Expand existing policies to cover areas of concern relating to who is authorized to use the equipment and check it out
3. Office manager will be in charge of 'releasing' the laptop for overnight only use.
6. Office manager will oversee implementation of encryption for data at rest

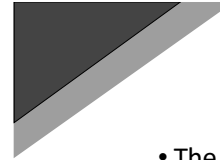
96





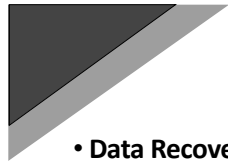
- **Who is going to follow up:**
- Office manager will assure that all components of the mitigation process are in place and functioning by \_\_\_\_\_, record the date of implementation on the risk analysis form and create a report detailing the new function to be placed in the hands of senior management by \_\_\_\_\_ (date).

97



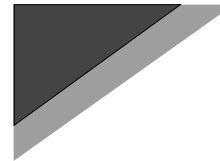
- The new wrinkle = Information Systems Activity Review
- Added request, in addition to risk analysis, started January 2015 as a new component of meaningful use attestation audits.

98



- **Data Recovery:** In the event of loss of access to data, for any reason, restoration can take place via Carbonite cloud backup. Senior management is in possession of the process for restoration.
- **Emergency Mode Function:** This piece of equipment is not critical for basic functions in the event of a disaster such as flood, earthquake, tornado, etc. that may interrupt or destroy function. Other office equipment can access needed data and perform functionality.

99



Clinic name  
 Address  
 City, State, ZIP

Service(s)	Reason Medicare May Not Pay:	Estimated Cost

**WHAT YOU NEED TO DO NOW:**

- Read this notice, so you can make an informed decision about your care.
- Ask us any questions that you may have after you finish reading.
- Choose an option below about whether to receive the service(s) listed above.

**Note:** If you choose Option 1 or 2, we may help you to use any other insurance that you might have, but Medicare cannot require us to do this.

**OPTIONS:** **Check only one box. We cannot choose a box for you.**

**OPTION 1:** I want the service(s) listed above. You may ask to be paid now, but I also want Medicare billed for an official decision on payment, which is sent to me on a Medicare Summary Notice (MSN). I understand that if Medicare doesn't pay, I am responsible for payment, but I can appeal to Medicare by following the directions on the MSN. If Medicare does pay, you will refund any payments I made to you, less co-pay or deductible.

**OPTION 2:** I want the service(s) listed above, but do not want Medicare. You may ask to be paid now as I am responsible for payment. I cannot appeal if Medicare is not billed.

**OPTION 3:** I don't want the service(s) listed above. I understand with this choice I am not responsible for payment, and I cannot appeal to see if Medicare would pay.

**Additional information:**

This notice gives you opinion, not an official Medicare decision. If you have other questions on this notice or Medicare billing, call 1-800-MEDICARE (1-800-633-4227TTY: 1-877-486-2046). Signing below means that you have received and understand this notice. You may ask to receive a copy.

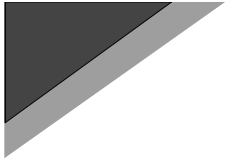
Signature: _____	Date: _____
------------------	-------------

You have the right to get Medicare information in an accessible format, like large print, Braille, or audio. You also have the right to be a caregiver if you find you've been discriminated against. Visit Medicare.gov/accessible for accessibility information.

Receiving this Advance Beneficiary Notice of Non-Coverage (ABN) does not mean you are not eligible for Medicare. Medicare will only pay for services that are covered under your Medicare plan. Medicare will not pay for services that are not covered under your Medicare plan. Medicare will not pay for services that are not covered under your Medicare plan. Medicare will not pay for services that are not covered under your Medicare plan. Medicare will not pay for services that are not covered under your Medicare plan.

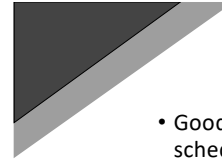
Form CMS-4311 (Rev. 03/11/2012) Form Approval OIGB No. 6031-0262

100



## Best Friend

101



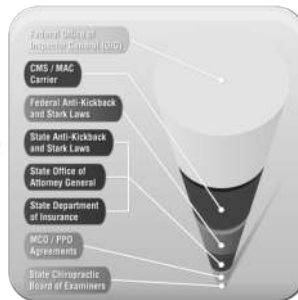
- Good place to pause and talk about compliant fee schedules for a second.
- When they look, they look...
- They look at forms, postings, what you have people sign and whether that info. is protected.
- Dual fee systems
- Point of service
- Now can NOT report to ins. if patient dictates, which can cause more scrutiny.

102

## How About You?...Do You Worry?

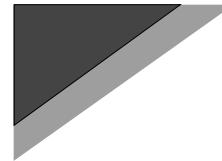
- Dual fee schedule?
- Cash discounts?
- OIG inducement violations
- Is your financial policy legal & compliant at all levels?

**If you don't worry, YOU SHOULD!**  
**Better yet. Know the Rules!**



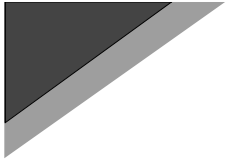
To receive a Sample 1 Page Financial Policy from Dr. Foxworth, Text **DRT** to (601) 227-7720. This is a great tool that you can customize in your office and a step toward becoming more compliant!

103



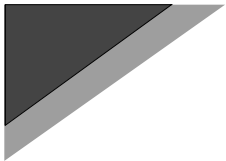
- State Attorney General Investigation

104



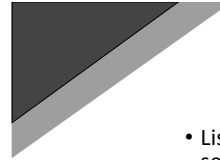
Subpoena:  
Provide documentation regarding:  
All services provided for past four years, to all patients, to include:

105



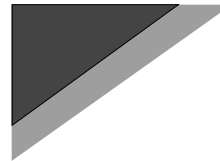
- If these different classification were charged differing rates for the CPT codes represented, what percentage be of each classification?

107



- List of all services provided, per patient, with each service identified by CPT code and identification which of the following classifications into which each individual would fall:
  - Identification of which of these consumers, involved in an accident, do not have a Lien
  - Identification of which of these consumers have not been involved in an accident and have no health insurance (or are not utilizing their health insurance)
  - Identification of which of these consumer have a Lien
  - Identification of which of these consumers have health insurance

106



- Provide details of discussions with patients, injury attorneys or outside referral companies regarding explanations of fees to be paid by patients in each classification...

108



109

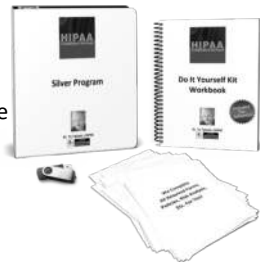
**Hands Off:** This is a very popular AFFORDABLE midrange service we provide for authoring your HIPAA compliance manual for you; Risk Analysis, ISAR, around 100 pages of policies, customized documents and forms, and much more required by the government. The promotional price is six payments of \$299 each or a \$100 discount for pay-in-full. If you have already purchased the DIY Kit, you will receive a credit toward your upgrade!

\*Additional DECREASED fee for Additional Clinics

**Super-Charge your Silver with HIPAA Boot Camp!**

With this Super-Charged Silver Program, you receive everything in both the DIY Kit & Silver program, plus we come on-site and train your compliance officer Face-to-Face. We assist with fully implementing your HIPAA program, train your staff in person, complete a physical plant walk through/inspection and Certify your Compliance Officer. Increase your six monthly payments to \$900 (Includes Travel Expenses) for HIPAA Boot Camp!

111



### Special Offer DIY Kit

- Retail Price of ~~\$549.00~~
- Discounted Webinar Price of **\$397.00**
- **7 Free Gifts** ( \$1200+ Retail Value!)

Call **214-437-7559** or  
 Email: [Ty.talcott@gmail.com](mailto:Ty.talcott@gmail.com) /  
[DrTyCompliance@gmail.com](mailto:DrTyCompliance@gmail.com)

110

### ***SEVEN (7) FREE GIFTS***

***included with the purchase of every HIPAA program!***

- OIG COMPLIANCE PROGRAM FOR FREE**  
(OIG Program DIY Manual; a \$399 value)
- TWO (2) FREE MONTHS OF MMM**  
(Mandatory Monthly Maintenance program; a \$58 value)
- REQUIRED ANNUAL STAFF TRAINING FOR FREE**  
(must be done within 45 days of each new hire; a \$185 value)
- ALERT LIST – FREE NEWSLETTER**  
(we continually provide law and enforcement changes plus updated compliance forms)
- OSHA – FREE DIY MANUAL**  
(includes training for a standard office; a \$159 value)
- NO SURPRISES ACT - FREE**  
(Templates, Instructions and GFE: *Good Faith Estimate*; a \$225 value)
- ONC – FREE Information Blocking Law**  
(Policies, Templates, and Instructions; a \$89 value)

112

- What You're Going To Get:**
- Complete HIPAA Compliance Manual..... (\$10,000 Value)
  - Mandatory Monthly Maintenance Program..... (\$2,000 Value)
  - Implementation Hand Hold Checklist..... (\$997 Value)
  - DIY HIPAA Program Workbook..... (\$547 Value)
  - HIPAA Compliance Customizer..... (\$4,000 Value)
  - BONUS: OIG Manual..... (\$400 Value)
  - Fast Action BONUS: Perfect Practice Solutions... (\$1,000 Value)
- Total Value: \$18,944



Get Started Now For Just  
**\$299/mo**  
 OR  
**\$99/mo**

PH: 214-437-7559 or  
[Ty.Talcott@gmail.com](mailto:Ty.Talcott@gmail.com) /  
[DrTyCompliance@gmail.com](mailto:DrTyCompliance@gmail.com)

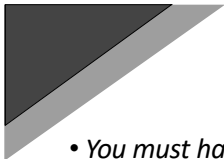
Get Started Now [DrTyTheComplianceGuy.com/go](http://DrTyTheComplianceGuy.com/go)

Hands-Off HIPAA Compliance

113

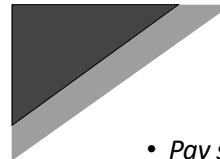


114



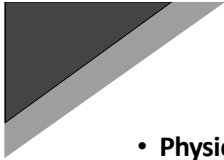
- *You must have policies/procedures relative to disposal of PHI records and all staff agree to abide by them. Need to document an audit trail to prove policies followed to complete destruction by outsourcing to a service, physically destroying or use of a software to sanitize (not recommended for USB/flash media due to sector sparing).*

115



- *Pay special attention to disposal of problem devices like printers, fax machines that store information, flash drives, etc. NIST, at government site, is a good resource for proper disposal.*

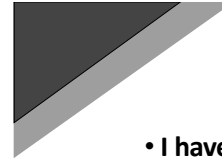
116



• **Physical access control**

*\*\* Policies must be in place and agreed to by staff, prescribing the physical safety and security of devices. All devices must be inventoried and accounted for. All computers are protected from environmental hazards. Physical access to secured areas is limited to authorized persons.*

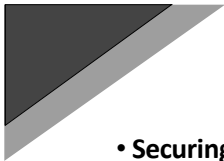
117



• **I have written a P & P to cover physical safety and security of devices and have a plan to enforce same.**

YES  
 NO

118

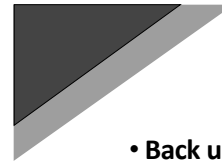


• **Securing electronic transmissions and network utilization**

*\*\*It is required to have integrity controls and encryption in place. Policies need to be in place prescribing network configuration and who has access and all staff agree to abide by them.*

• *Access is restricted to authorized users and devices. Guest devices may not contain PHI, no peer- to peer applications. No public instant messaging and private instant messaging-only if secured.*

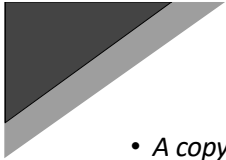
119



• **Back up and Securing Encryption methods for offsite electronic media, backup tapes, data at rest, text messaging, etc.**

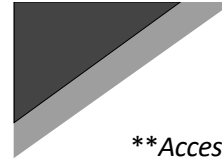
*\*\*Back up...policies and procedures for backup and recovery are in place and agreed to by staff, all staff understand their duties during recovery. The entire system restore process is known to at least one person outside the practice.*

120



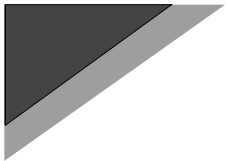
- *A copy of recovery plan is safely stored offsite, files that are critical are documented and listed in the backup configuration. There is a timely and regular backup schedule and every run is tested for its ability to restore data accurately. Backup media are secured or encrypted- if offsite. Back ups are unreadable prior to disposal. Multiple backups are maintained*

121



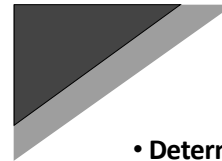
*\*\*Access control policies must be in place and all staff agree to abide by (document this). What to do at termination of employee, every user account must be documented to be tied to a currently authorized individual, minimum necessary states an individual may only access what is needed to perform their work, all files must be set to allow only authorized individuals to use. Computers running health care data are not allowed for other uses.*

122



- Awareness training relative to these and all other issues is required (annual and ongoing).

123



• **Determining which audit logs to activate**

- Only the audit logs you will actually use and monitor are appropriate to be activated. Choosing which audits to have open is based on risk and sensitivity of data.

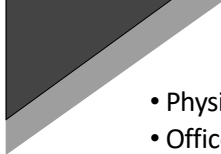
124



- **Auditing your use of logins/trails**

- Tracking must contain, at the least, personal ID, date, time, reason accessing (view, change, delete) and show all attempts- successful and unsuccessful.
- Your logins should time out/lock out after three attempts. There should be written reports in your HIPAA manual relative to summary of logs and sanctions in place for violations.

125

- 
- Physical Plant “Walk Through” Audit
  - Office: \_\_\_\_\_ Date: \_\_\_\_\_
  - **Area of review**
  - **Compliant - Y/N**
  - **Comments**
  - Patient charts located in secure area. **Y/N**
  - Names on charts protected. **Y/N**

126

- 
- Information at front desk protected.

**Y/N**

- Insurance/Collection calls not able to be heard from patient area.

**Y/N**

- Computer screens with rapid time out/password protected.

**Y/N**

127

- 
- Sign in sheet does not contain health information.

**Y/N**

- Phone messages kept in protected area.

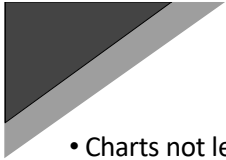
**Y/N**

- Charts not left in unprotected areas of office with identifiable information visible.

**Y/N**

128





- Charts not left in exam or treatment areas after patient treatment.

**Y/N**

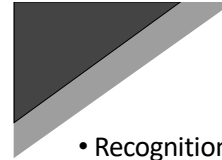
- X-rays/other diagnostic tools removed after patient treatment from examination/ treatment area.

**Y/N**

- Patient information and treatment not discussed in common areas.

**Y/N**

129



- Recognition boards/pictures etc. do not include identifiable information.

**Y/N**

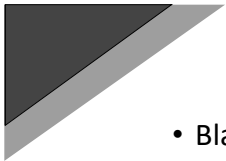
- Privacy provided as needed based on treatment provided.

**Y/N**

- Patient Rights accessible upon request. Staff knowledgeable about location.

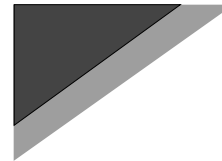
**Y/N**

130




- Blackout screens
- Computer Passwords
- Rapid time out screensavers
- Relocation of Computers
- Relocation of staff member
- New Sign In sheet

131



Required In-Service

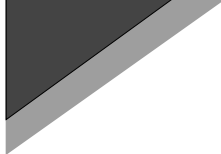
132



Here are some key points for your required In-Service.

- History of HIPAA
- Benefits of Compliance With The Privacy Laws
- Why do we need to be compliant?
- The Privacy Rule: Who Is Affected

133

- 
- Our Compliance/Privacy Officer is: \_\_\_\_\_
  - Our Privacy Rules can be reviewed by patients, the policy is located \_\_\_\_\_.
  - No records are faxed, or mailed from the office unless the Compliance /Privacy Officer is notified so that proper consents and procedures can be followed.
  - All patient information is considered private, therefore staff is expected to:
    - Make sure all records are kept confidential and out of sight.
    - Patients are not discussed outside the office
    - Phone conversations are kept private and not held where other patients can hear sensitive information.

134



This office will destroy records in the following manner:

1. Burn or
2. Shred
3. Outside company

*Documentation will be kept of all records destroyed and the manner of destruction.*

This office will secure records in the following manner:

- 1.
- 2.

135



*Disciplinary Standards & Enforcement*

136

### *Release of Patient Information*

Confidential information includes:

- Any communication between a patient and the doctor.
- Any communication between a patient and other clinical persons regarding:
- All clinical data, i.e., diagnosis, treatment; Patient transfer to a facility for treatment of drug abuse, alcoholism, mental/psychiatric problem;

137

### *Telephone Requests for Release of Confidential Patient Information*

- Medical information regarding a patient shall not be released over the telephone except when required for **immediate** patient care.

138

### *Fax Requests for Release of Confidential Patient Information*

- Authorization for release of medical information will be accepted through a fax machine (hardcopy is preferred). Information will be faxed to **physicians' offices only** and **only** in emergency cases and/or when the patient is in the office.

139

### "Hands-Off HIPAA Compliance" is all about



- Helping you Install and Maintain your HIPAA program in as little time as possible...
- So you can focus on your practice
- So you can help and protect your patients
- So you can practice stress-free knowing you have a defensible position

Hands-Off HIPAA Compliance

140

## Here's What You Get...

141

Hands-Off HIPAA Compliance

### "But Dr. Ty, I Have A HIPAA Program!"

- Do you have everything we just went over?
- Do you have and did you sign off on a risk analysis, mitigation plan and at least four ISAR's in the last year?
- Do you have and did you SIGN OFF on, about a dozen HIPAA reviews, evaluations and audits in the last year (about one per month)?
- Did you issue a security reminder to your staff last month and have one ready for this month?
- In my experience 99% of practices don't have everything they need

143


Hands-Off HIPAA Compliance

## "Complete HIPAA Compliance Manual"

- We author your HIPAA compliance manual for you: Risk Analysis, ISAR, around 100 pages of policies, customized documents and forms, and much more!
- Everything you need to be compliant (usually 300–800 pages)
- We send you a questionnaire, you answer it and we put together your manual based on what your practice needs. (It's different for everyone)
- We have it in Digital Format
- Also Physical copy as well.

142

Hands-Off HIPAA Compliance



### **SEVEN (7) FREE GIFTS** *included with the purchase of every HIPAA program!*

**OIG COMPLIANCE PROGRAM FOR FREE**  
(OIG Program DIY Manual; a \$399 value)

**TWO (2) FREE MONTHS OF MMM**  
(Mandatory Monthly Maintenance program; a \$58 value)

**REQUIRED ANNUAL STAFF TRAINING FOR FREE**  
(must be done within 45 days of each new hire; a \$185 value)

**ALERT LIST – FREE NEWSLETTER**  
(we continually provide law and enforcement changes plus updated compliance forms)

**OSHA – FREE DIY MANUAL**  
(includes training for a standard office; a \$159 value)

**NO SURPRISES ACT - FREE**  
(Templates, Instructions and GFE: *Good Faith Estimate*; a \$225 value)

**ONC – FREE Information Blocking Law**  
(Policies, Templates, and Instructions; a \$89 value)

144

"I have to say I love Dr. Ty Talcott's MMM Program. It has made my life so much easier along with my HIPAA compliance.

I get the form(s) emailed to me every month, so I don't even have to worry about it. I just follow the directions, complete the form and file in my HIPAA manual.

Well worth the monthly fee! Thank you Dr. Ty!"



Dr. Kristine Springer

## We've Got Your Back Guarantee

- If you are ever audited... We've got your back
- We'll fight with you. Tell you what to do, what not to do and help you navigate the whole thing

Get Started Now [DrTyTheComplianceGuy.com/go](http://DrTyTheComplianceGuy.com/go)

### What You're Going To Get:

- Complete HIPAA Compliance Manual..... (\$20,000 Value)
- Mandatory Monthly Maintenance Program..... (\$2,000 Value)
- Implementation Hand Hold Checklist..... (\$997 Value)
- DIY HIPAA Program Workbook..... (\$547 Value)
- HIPAA Compliance Customizer..... (\$10,000 Value)
- BONUS: OIG Manual..... (\$400 Value)

Total Value: \$33,944

Get Started Now For Just

**\$299/mo**  
for 6 months



Get Started Now [DrTyTheComplianceGuy.com/go](http://DrTyTheComplianceGuy.com/go)



## Special Offer DIY Kit

- Retail Price of ~~\$549.00~~
- Discounted Webinar Price of **\$397.00**
- 7 Free Gifts ( \$1200+ Retail Value!)

Call 214-437-7559 or

Email: [Ty.talcott@gmail.com](mailto:Ty.talcott@gmail.com) /  
[DrTyCompliance@gmail.com](mailto:DrTyCompliance@gmail.com)

149

### What You're Going To Get:

- Complete HIPAA Compliance Manual..... (\$10,000 Value)
- Mandatory Monthly Maintenance Program..... (\$2,000 Value)
- Implementation Hand Hold Checklist..... (\$997 Value)
- DIY HIPAA Program Workbook..... (\$547 Value)
- HIPAA Compliance Customizer..... (\$4,000 Value)
- BONUS: OIG Manual..... (\$400 Value)
- Fast Action BONUS: Perfect Practice Solutions... (\$1,000 Value)

Total Value: \$18,944



150

Get Started Now For Just

**\$299/mo**

**OR**

**\$99/mo**

PH: 214-437-7559 or

[Ty.Talcott@gmail.com](mailto:Ty.Talcott@gmail.com) /  
[DrTyCompliance@gmail.com](mailto:DrTyCompliance@gmail.com)

Get Started Now [DrTyTheComplianceGuy.com/go](http://DrTyTheComplianceGuy.com/go)

Hands-Off HIPAA Compliance