WCA
Wisconsin Chiropractic Association

Special Presentation:
HIPAA Survival

Dr. Ty Talcott, CHPSE
C: 469.371.8804 / PH: 214.437.7559
Ty.talcott@gmail.com / Info.hipaa@gmail.com

- Foxworth Video

A Little about me.

Ski Lift Acrobatics

How do they catch people

Head of Georgia legislative committee – Human Error

Paper protection – practice sale

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

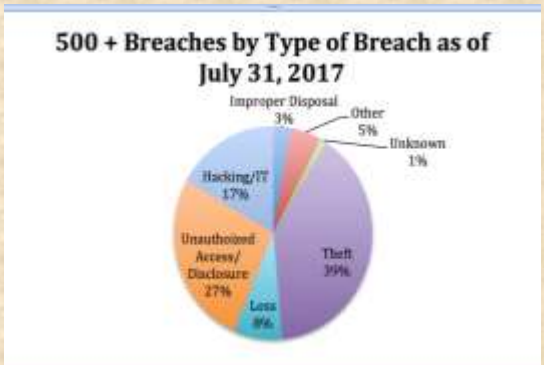
Patient Complaints

My Buddy

1 – 2 - 3

Cyber-security / Ransom Ware

- Ledet Video



So, what do they do with the information?
ID theft, ins. cards, devices..
Tax returns
So, what did the government do about physician office compliance?

Direct from HIPAA conference
Washington DC - Sept. 2017
* Virtually every Doctor hit with
an attack/breach says the same thing,
"I thought it would never happen to me!!"

* 2017 HIPAA complaints that must be investigated by OCR, will easily top 20K in 2017 up **300%** since 2011!!!

Huge breaches:
Target and pharmacies
Anthem Insurance = 80 million breached
Blue Cross Perma Blue = 11,000,000 breached
Now Largest HIPAA fine = 115

U.S. Department of Health and Human Services
Office of Inspector General

MEDICARE NEEDS BETTER CONTROLS TO PREVENT FRAUD, WASTE, AND ABUSE RELATED TO CHIROPRACTIC SERVICES

February 2018

An OIG Portfolio

A-09-16-02042

This portfolio presents an overview of program vulnerabilities identified in prior Office of Inspector General (OIG) audits, evaluations, investigations, and legal actions related to chiropractic services in the Medicare program. It consolidates the findings and issues identified in that work and discusses recommendations from prior reports that have not been implemented or have been implemented ineffectively. In addition, this portfolio provides information to help the Centers for Medicare & Medicaid Services understand the need for effective controls over chiropractic services and offers recommendations to help Medicare prevent fraud, waste, and abuse related to those services.

The OIG work referenced throughout this portfolio was conducted in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency, generally accepted government auditing standards, and investigative and legal professional standards, as applicable.

Here are some chilling quotes taken from the official report.

"This portfolio presents an overview of program vulnerabilities related to chiropractic services in the Medicare program.

In addition, this portfolio offers recommendations to help Medicare prevent fraud, waste, and abuse related to those services.

The Centers for Medicare & Medicaid Services' (CMS's)
Comprehensive Error Rate Testing program,
...identified chiropractic services as having the highest improper payment rates among Medicare [providers]...

* The improper payment rate ranged from 43.9 percent to 54.1 percent, and overpayments per year ranged from $257 million to $304 million.

CMS has not implemented .. all of our recommendations, and controls over chiropractic services remain inadequate to prevent fraud..

This.. illustrates the need for better controls .. to prevent beneficiaries from paying millions of dollars in coinsurance for chiropractic services that are not reasonable or necessary... chiropractic services that are not reasonable or necessary can potentially harm Medicare beneficiaries

Action Needed:
educate beneficiaries on the types of chiropractic services covered by Medicare, inform them that massage and acupuncture services are not covered ., and encourage them to report to CMS chiropractors who are providing non-Medicare-covered services;

* Chiropractors should be forced to refund amounts overpaid by Medicare;

* Establish a threshold for the number of chiropractic services paid .

* Establish a more reliable control for identifying active treatment.
(you need to be plugged into updates)

Implement medical review for preauthorizing certain chiropractic services.

. To provide CMS additional data, we conducted our CY 2013 nation-wide review, which found an 82 percent improper payment rate, resulting in $358.8 million in overpayments.. Specifically, services in excess of 30 per beneficiary per year were all unallowable.

. In addition, our investigations and legal actions demonstrated that chiropractic services were susceptible to Medicare fraud. (note: here is a where an OIG program is critical)

So, what do we do about it?

OIG compliance program is about having a system in place to assure that clinics filing to a federal program do so error/fraud free.

The OIG seven step process:

1. Written policies—code of ethics, documentation, etc….
2. Compliance officer
3. Training
4. Effective communication
5. Auditing
6. Enforcement
7. Detecting offenses

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!

Overview of what a HIPAA Regulatory Compliance Manual Looks Like

[Clinic Name]

Index

1. Compliance Officer

Job Description

Notification of Officer Appointment/Posting

Policy and Procedure

Filing a complaint

2. Notice of Patient Privacy Policy - 2013 Omnibus Rules, Increased enforcement and fines

3. Forms

Consent to use PHI

Restricted Consent

Patient Authorization

Revocation of Authorization

Approve Request to Copy

Deny Request to Copy

4. Required Accounting Log – per patient

5. Corrective Action Forms

6. Employee Confidentiality Statements

7. Business Associate Confidentiality Contracts - 2013 Omnibus Rules, Increased enforcement and fines

8. Annual required Staff In-service training - privacy and security rules.

9. Physical Plant Audit

10. Risk Analysis

11. ISAR

12. Required Annual A-Z HIPAA program Audit/Evaluation

13. BONUS Audits

- Claim Denial Review
- Medicare ABN Compliance
- Clinical File Review

14. Policies and Procedures for Security Rules

15. Required Contingency plan with data recovery and emergency mode operations

16. Required equipment maintenance log

17. Model release for testimonial use

18. Audit Schedule for 2017

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

- Audit Schedule Detail

BUSINESS ASSOCIATE AGREEMENT

PROTECTIVE PERSONAL HEALTH INFORMATION

This Business Associate Agreement ("Agreement") is made and entered into this _____ day of _____, 20__, by and between _____ ("Business Associate"), and _____ ("Covered Entity"), a _____, which maintains its principal place of business at _____.

WHEREAS, Business Associate is a vendor for Covered Entity;

WHEREAS, Covered Entity is a provider of health care services and possesses and maintains certain confidential Private Health Information;

WHEREAS, Covered Entity and Business Associate have agreed to conduct all of their business in compliance with HIPAA Standards.

Section 1
Definitions

"**Privacy Rule**" shall mean the Standards for Privacy of individually identifiable health information at 45 CFR Part 160 and Part 164, Subparts A and E.

"**Protected Health Information**" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

"**Secretary**" shall mean the Secretary of the Department of Health and Human Services or his designee.

Section 2
Obligations of Business Associate

During the Agreement Term, Business Associate agrees to:

- Not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law.
- Use appropriate safeguards to prevent use or disclosure of Protected Health Information as needed other than as provided for by this agreement.
- Report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
- Ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement.
- To make internal practices, books and records and disclosure of Protected Health Information received from, or created or received by Business

Privacy Posting Changes

- Privacy Posting is now called the "Notice of Patient Privacy Policy"
- The Policy must include that you need special releases for:
- disclosures of psychotherapy notes
- disclosures of Protected Health Information for marketing purposes; and
- disclosures that constitute a **sale** of Protected Health Information; as well as a statement that other uses and disclosures not described in the Notice of Privacy Practices will be made only with authorization from the individual.

- That an individual has a right to opt out of fundraising communications (i.e. if the Covered Entity intends to contact the individual regarding fundraising).
- The right of an affected individual to be notified following a breach of unsecured Protected Health Information.

- Email Form
- Alert List
- CHUSA
- Affordable Care Act (Obamacare)
- Guides

Best Friend

Patient Name: **Identification Number:**

Advance Beneficiary Notice of Noncoverage (ABN)

NOTE: If Medicare doesn't pay for services below, you may have to pay. Medicare does not pay for everything, even some care that you or your health care provider have good reason to think you need. We expect Medicare may not pay for the **service** below.

Services	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 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 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-pays or deductibles.

☐ **OPTION 2.** I want the service listed above, but do not bill 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** 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 our opinion, not an official Medicare decision. If you have other questions on this notice or Medicare billing, call **1-800-MEDICARE** (1-800-633-4227/**TTY:** 1-877-486-2048). Signing below means that you have received and understand this notice. You also receive a copy.

Signature:	Date:

CMS does not discriminate in its programs and activities. To request this publication in an alternative format, please call: 1-800-MEDICARE or email: ABFormatRequest@cms.hhs.gov.

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0566. The time required to complete this information collection is estimated to average 7 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Baltimore, Maryland 21244-1850.

Form CMS-R-131 (Exp. 03/2020) Form Approved OMB No. 0938-0566

Risk Analysis

- **Risk Analysis**
- **Date performed_____**
  Participants_____
- **Inventory of Assets that contain PHI, including key staff, business associates, etc. :**
  - **Lap Top Computer**
  - **On-site server**
  - **_____, etc.**

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.

- **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

- **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

- **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.

7. A 'check out system' could be set up similar to a library card
8. One individual could be put in charge of 'loaning out' equipment and keeping a log of who has what, where, etc.
9. Could require the lap top never leave the office.
10. Check with IT professional for encryption solutions
11._____, etc.

- **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 lap top for overnight only use.

6. Office manager will oversee implementation of encryption for data at rest

- **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).

- 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.

- **Equipment Maintenance:** Equipment is maintained by in-house IT staff_____(name of person/persons). Any outside work needed is monitored by such person as who did what at what time and is recorded on the risk analysis form for easy review and update- as well- status of periodic testing for proper function of maintained equipment if recorded.

- **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.

Which chiropractors are at risk if they do not provide translation services for 15 top, non-English languages for their patients to satisfy the new law enacted October 16 of this year?

- *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).*

- *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.*

- **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.*

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

__YES

__NO

- **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.*

- **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.*

- *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*

***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.*

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

- **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.

- **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.

- 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

- 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

- 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

- 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

- 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

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

Required In-Service

- 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

- 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.

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.

Disciplinary Standards & Enforcement

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;

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.

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.