# Back To Chiropractic Continuing Education Seminars

# HIPAA Compliance for the Chiropractor ~ 2 Hours

**Welcome:**

**This course counts as 2 Hours of CE for HIPAA Compliance for the Chiropractor for the Chiropractic Board of Examiners for the state of California.**

**There is no time element to this course, take it at your leisure. If you read slow or fast or if you read it all at once or a little at a time it does not matter.**

## How it works:

1. **Helpful Hint: Print exam only and read through notes on computer screen and answer as you read.**
2. **Printing notes will use a ton of printer ink, so not advised.**
3. **Read thru course materials.**
4. **Take exam; e-mail letter answers in a NUMBERED vertical column to marcusstrutzdc@gmail.com.**
5. **If you pass exam (70%), I will email you a certificate, within 24 hrs, if you do not pass, you must repeat the exam. If you do not pass the second time then you must retake and pay again.**
6. **If you are taking the course for DC license renewal you must complete the course by the end of your birthday month for it to count towards renewing your license. I strongly advise to take it well before the end of your birthday month so you can send in your renewal form early.**
7. **Upon passing, your Certificate will be e-mailed to you for your records.**
8. **DO NOT send the state board this certificate.**
9. **I will retain a record of all your CE courses. If you get audited and lost your records, I have a copy.**

**The Board of Chiropractic Examiners requires that you complete all of your required CE hours BEFORE you submit your chiropractic license renewal form and fee.**

**NOTE: It is solely your responsibility to complete the course by then, no refunds will be given for lack of completion.**

**Enjoy,**

**Marcus Strutz DC**

**CE Provider**

**Back To Chiropractic CE Seminars**

# HIPAA COMPLIANCE for the Chiropractor

Michelle Massa, DC, CEES

# Introduction

- Education & Background
  - Psychology, Lifestyle, Nutrition & Wellness
    - Neuropsychology & Behavioral Psychology
    - Health Education – Adult Weight Management
  - HIPAA, Ethics and Law, History, Exam, Diagnosis & Documentation
    - Compliance Officer – Life West Health Center
  - Certified Ergonomist
    - Ergonomic Evaluations
    - Ergonomic & Workplace Safety Trainings
- www.MichelleJMassa.com

# Goals & Objectives

- Review HIPAA
- Have an adequate understanding of Protected Health Information & Accessibility
- Understand the components of a HIPAA compliant chiropractic office

# Overview

- HIPAA
  - The Privacy Rule
  - The Security Rule
- HIPAA according to Federal Regulations
- How to maintain a HIPAA compliant chiropractic practice in the state of California

# What is HIPAA

- Health Insurance Portability and Accountability Act
- HIPAA Sets a National Standard
  - To ensure both the proper access to and confidentiality of medical records, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
  - HIPAA is a federal law that establishes the rules for managing medical information throughout the United States. Although states may adopt stricter confidentiality rules, HIPAA sets the minimum standards and protections for medical privacy.
- HIPAA is a program designed by the federal government to ensure that patient's health records are kept confidential

# What does HIPAA Protect

- Protects patients privacy
  - Visual privacy
  - Auditory privacy
  - Prevents unauthorized access

# HIPAA History

- To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
- Required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security.
- At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information.
- Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

# HIPAA History

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002.
- This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: **health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.**
  - Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final Security Rule in February 2003.
  - This Rule sets national standards for protecting the confidentiality, integrity, and availability of **electronic protected health information.** Compliance with the Security Rule was required as of April 20, 2005

# Covered Entities

- HIPAA's privacy and security rules must be followed by "covered entities." These include any person or business that provides, bills, or receives payment for medical care, including:
  - health care providers
  - clearinghouses that process (change the format of) medical information
  - health plans and health insurance issuers

# Business Associates

- HIPAA also covers "business associates" who have access to health care information from covered entities.
- "Business associates" are individuals and organizations (including contractors and other non-staff) who perform certain services and activities, such as:
  - claims processing and third-party billing
  - administrative, management, and professional consulting
  - data transmission, storage, and aggregation (including web-hosting)

# The Privacy Rule

- The HIPAA Privacy Rule:
  - protects individually identifiable health information
  - requires organizations to establish safeguards to ensure medical privacy
  - restricts the use and disclosure of medical information
  - gives patients the right to access and control their medical records

# The Privacy Rule

- The HIPAA Privacy Rule requires organizations to:
  - adopt privacy policies and procedures
  - notify patients and clients about their privacy rights
  - institute safeguards to secure Protected Health Information (PHI)
  - train staff (employees and volunteers) on their responsibility for privacy
  - appoint a Privacy Officer responsible for enforcing privacy requirements
  - set up procedures to respond to complaints about privacy
  - take steps to minimize any unauthorized access or use of PHI

# The Privacy Rule

- The Privacy Rule protects health information from the time a record is created (or the information is revealed) to the time it's destroyed.
- Generally, covered entities and business associates may not use or release an individual's medical information unless the Privacy Rule expressly permits it, or the individual authorizes it.
- And when medical information may be shared, the Privacy Rule strictly limits the amount of information that may be provided.

# The Privacy Rule

- The Privacy Rule does not forbid all disclosures of medical data. For example, there are almost no restrictions on providing information to:
  - the patient
  - someone authorized by the patient
  - a health care professional treating the patient

# Protected Health Information (PHI)

- Because HIPAA is designed to protect personal privacy, the Privacy Rule applies to any "individually identifiable health information."
- Thus, any information or record, in any form or media (including electronic, paper, or oral), about an individual's mental or physical health, condition, or treatment (whether past, present, or future), should be considered **Protected Health Information** (PHI).

# De-Identified PHI

- **De-Identified PHI**
  One way to avoid HIPAA's limitations (and simultaneously protect patients' privacy) is to "de-identify" medical records or other PHI.
  - For example, PHI can be de-identified by taking out all information that can be linked to any individual; the remaining data is then de-identified.

# Minimum Necessary

- The **Privacy Rule** generally requires covered entities to take **reasonable** steps to limit uses, disclosures, or requests (if the request is to another covered entity) of **protected** health information (PHI) to the minimum necessary to accomplish the intended purpose.

# Protected Health Information (PHI)

- According to HIPAA, medical records and data are PHI when they contain "individual identifiers" such as:
  - names
  - contact information (street or email address, telephone or fax number)
  - dates directly relating to an individual (birth or death, admission or discharge)
  - geographic subdivisions smaller than a state (county, city, zip code)
  - account numbers (Social Security, medical record, insurance)
  - biometric identifiers (fingerprint, retinal scan, full-face photograph)
  - other unique identifiers (certificate or license number, vehicle license plate, Web URL, IP address)
- By contrast, if information doesn't relate to specific people (such as a hospital's annual occupancy rate), it probably isn't PHI.

# Accessibility and Authorized Disclosures

- Although HIPAA ordinarily restricts sharing health information, it **requires** organizations to disclose PHI in two situations:
  - when an individual (or their personal representative) requests their own information
  - to respond to investigations by the Department of Health & Human Services

# Patient Requested Restrictions

- HIPAA also allows individuals to request restrictions on future uses of their PHI. Basically, patients can ask to limit the type or amount of information an organization will provide. For example, a patient may ask:
  - that certain relatives not be informed about the patient's condition
  - for communications to alternative or specific addresses (that bills be sent to a post office box, or that calls be made to a cell phone rather than to a home telephone number)
  - for confidential communications (appointment reminders mailed in a sealed envelope rather than a post card, or that no messages be left on an answering machine)
  - that health plans not be told about treatments if the patient pays for the service in full
  - for other specific restrictions on the use of their PHI

# Individual Rights

- HIPAA also gives individuals control over their own PHI, including the right to:
  - access their PHI
  - obtain copies of their PHI (including electronic records) within 30 days
  - request amendments to correct or complete their records
  - request confidential communications
  - obtain an accounting of who used or received their PHI
  - impose restrictions on disclosure of their PHI under certain conditions
  - opt out of fundraising communications
  - revoke previous authorizations
  - file complaints

# Incidental Disclosures

- HIPAA requires organizations to protect medical privacy. However, even with precautions, there is always the possibility of an "incidental" disclosure.
- Still, it's important to be aware of the risk of (and guard against) incidental disclosures. For example:
  - speak quietly when discussing patients or health care in public areas (waiting room, hallways, elevators)
  - avoid using patients' names in public areas
  - use a private office when authorized to discuss PHI on the telephone
  - don't leave health care records or files where they're visible to others

# How can you Protect Patient Confidentiality

- Minimize Incidental Disclosures
- Sign in Sheets
- Check in line/Check out Line
- Limit discussions in waiting rooms
- Stay away from specific conversations in hallways
- Speak in low tone in open areas
- Telephone practices

# Security Rule

- The Security Rule applies to health care information (including handling claims or determining eligibility) involving electronic data:
  - in transit across the Internet, intranet, and wireless networks
  - downloaded to a smartphone, tablet, or other mobile device
  - at rest in electronic media such as magnetic tape, disks, CDs, etc.
  - in use while electronic records are created, updated, or retrieved
  - being destroyed (e.g., disks being erased, recycled, or disposed of)
- The Security Rule even applies when E-PHI is moved physically, such as when someone carries around a disk, flash drive, or a laptop computer.

# Electronic Protected Health Information (E-PHI)

- The Security Rule applies to health care information (including handling claims or determining eligibility) involving electronic data:
  - in transit across the Internet, intranet, and wireless networks
  - downloaded to a smartphone, tablet, or other mobile device
  - at rest in electronic media such as magnetic tape, disks, CDs, etc.
  - in use while electronic records are created, updated, or retrieved
  - being destroyed (e.g., disks being erased, recycled, or disposed of)
- The Security Rule even applies when E-PHI is moved physically, such as when someone carries around a disk, flash drive, or a laptop computer

# Electronic Protected Health Information (E-PHI)

- The Security Rule requires organizations to implement safeguards for electronic Protected Health Information (E-PHI), including:
- **Administrative safeguards**, such as assigning responsibility for security and appointing a "Security Official," adopting procedures to prevent and correct security violations, providing security training to staff, and disciplining staff for security policy violations.
- **Physical safeguards**, which are methods to protect data, equipment, and the facility against physical hazards (backing up data off-site and requiring laptops to be locked when not in use) and to prevent unauthorized use or intrusion (locking office doors, and erasing disks before reusing them).
- **Technical safeguards**, which are primarily automated procedures to track and reduce unauthorized access (computer log-in and automatic log-off procedures, requiring special verification procedures for offsite/remote log ins, and authentication controls ensuring data encryption during transmission).

# How to Make Web-Forms HIPAA Compliant

- Some of the more popular web-forms on the market include JotForm, Ninja Forms, WuFoo, Gravity Forms, and Contact Form 7.
- Several of these forms are WordPress plug-ins and extensions that allow users to place web-forms directly onto their site.
- You won't find HIPAA compliant online forms, but you *can* use these services in a manner that conforms to HIPAA regulation.

# How to Make Web-Forms HIPAA Compliant

- First and foremost: ask your web-form service if they'll sign a **Business Associate Agreement** to legally protect your patients' data.
- Make sure that you're creating encrypted forms.
  - Encryption allows you to keep data more secure. Encrypted web-forms will guard any data entered into them so that they can only be accessed by entering a key.
  - End-to-end encryption is the most secure and should be your preferred choice.

# How to Make Web-Forms HIPAA Compliant

- Regularly download encrypted data, store it on a secure internal server, and then delete the data from the web-form's servers.
- Always logout of your web-form service when you've completed your session.
- By implementing these important privacy and security measures when addressing HIPAA for web-forms, you're making a step toward protecting patients' PHI.

# HIPAA forms

- Notice of Privacy Practices
- Patient Acknowledgement/Receipt of the Notice
- Business Associate Agreement
- Consent Form
- Authorization Form
- Fax Cover Sheet
- Media Consent Form

# Privacy Practices Notice

- Besides protecting medical privacy, HIPAA also requires organizations to notify individuals about their rights.
- Most organizations meet this requirement by distributing a Privacy Notice. These notices must clearly explain:
  - the organization's privacy practices and obligations
  - how the organization may use and disclose PHI
  - the organization's duty to provide notice about breaches of PHI (discussed later)
  - the uses and disclosures of PHI that require authorization
  - their rights to complain and whom to contact

# Records and Logs

- At the ROF: “I love seeing my x-rays. Can I take a picture of these on my phone?”
- Maintain a log of all records released
  - Name
  - Patient number
  - Date requested
  - Date processed/released
  - Where/Who
    - Name, address, phone, fax, email

# Communications

- Email
  - Email communications are permitted, but you must take precautions
  - It is a good idea to warn patients about the risks of using email that includes patient health information (PHI)
  - Providers should be prepared to use email for certain communications, if requested by the patient, but must ensure they are not exposing information the patient does not want shared
  - Providers must take steps to protect the integrity of information and protect information shared over open networks

# Email Communication sample

- Sample Email Confidentiality Notice WARNING: CONFIDENTIALITY NOTICE - The information enclosed with this transmission are the private, confidential property of the sender, and the material is privileged communication intended solely for the individual indicated. If you are not the intended recipient, you are notified that any review, disclosure, copying, distribution, or the taking of any other action relevant to the contents of this transmission are strictly prohibited. If you have received this transmission in error, please notify us immediately at (xxx) xxx-xxxx or xxxx@xxxxxxx.com.

# Email & Text Communication sample

- Regulations require encrypted messaging systems for confidential communications. Since our e-mail/text communications are not encrypted, it is the policy of [Practice Name] not to use e-mail/text for sharing confidential information. We are sorry if this causes inconvenience for you in receiving information from us. Please call us at (xxx)xxx-xxxx. Further information about our practice can be found on our website at www.xxxxxxx.com
- If you have a medical emergency, please dial 911.

# Social Media and Yelp

- Online
  - Facebook, Instagram, Twitter, etc.
    - Understand that even a deleted post can still exist in cyberspace.
    - Search engines are constantly scouring all social channels, aggregating and storing information to serve it up to anyone entering a search query. If a few seconds pass between posting a comment and deleting it, the search engine may have already come, picked up the information and gone.
    - Understand that even if a patient posts every last detail about his or her medical issues and treatments, no medical professional or staff should repost, retweet or "regram" this information on their personal pages.
  - Yelp
    - Any acknowledgement = HIPAA violation

# Patient Testimonials

- Create & Implement a HIPAA Media Release Form
  - There may be certain circumstances where you wish to share a patient testimonial or answer a question.
  - It's important to have the patient's **written consent** before posting.
  - If it is a video testimonial, know that the patient may rescind authorization at any time.
  - If it is photo of them with a statement regarding their condition, make sure you have the written authorization & know that the have the right to rescind authorization at any time.

# HIPAA Sanctions

- HIPAA also specifically requires an employer to "apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures" [45 CFR §164.530(e)]. Thus, organizations are required by law to discipline staff for violating HIPAA's privacy regulations.

# Case Example – Social Media

- In 2011, the Board of Nursing delivered a warning to a nurse who commented on a small town newspaper's blog. The nurse discussed a patient in positive terms using a nickname. Even though she did not mention the patient's real name or medical issue, mentions of his age and mobility aids made it clear which member of this small town the nurse was treating. HIPAA specifies 18 items beyond just a patient's name that must remain private. The nurse violated the patient's privacy rights, threatening her standing and position.

# Case Example – Social Media

- In an incident with particularly harsh repercussions, a student nurse moved by her three-year-old chemotherapy patient's bravery took a photo of the boy and posted it on her Facebook page. Even though she had privacy settings in place, another nurse not among that student nurse's Facebook friends came across the post and photo. This nurse informed the hospital. This HIPAA violation got the student nurse expelled from the nursing program and the nursing program bounced off of that hospital's list of accepted schools from which to draw student nurses. Even when motivated by the best intentions, HIPAA violations can result in severe consequences.

# Case Examples
# Minimum Necessary/Confidential Communications

- A hospital employee did not observe minimum necessary requirements when she left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. An OCR investigation also indicated that the confidential communications requirements were not followed, as the employee left the message at the patient's home telephone number, despite the patient's instructions to contact her through her work number. To resolve the issues in this case, the hospital developed and implemented several new procedures. One addressed the issue of minimum necessary information in telephone message content. Employees were trained to provide only the minimum necessary information in messages, and were given specific direction as to what information could be left in a message. Employees also were trained to review registration information for patient contact directives regarding leaving messages. The new procedures were incorporated into the standard staff privacy training, both as part of a refresher series and mandatory yearly compliance training.

# Case Examples – Access

- A patient alleged that a covered entity failed to provide him access to his medical records. After OCR notified the entity of the allegation, the entity released the complainant's medical records but also billed him $100.00 for a "records review fee" as well as an administrative fee. The Privacy Rule permits the imposition of a reasonable cost-based fee that includes only the cost of copying and postage and preparing an explanation or summary if agreed to by the individual. To resolve this matter, the covered entity refunded the $100.00 "records review fee."

# Case Examples – Uses & Disclosures

- A public hospital, in response to a subpoena (not accompanied by a court order), impermissibly disclosed the protected health information (PHI) of one of its patients. Contrary to the Privacy Rule protections for information sought for administrative or judicial proceedings, the hospital failed to determine that reasonable efforts had been made to insure that the individual whose PHI was being sought received notice of the request and/or failed to receive satisfactory assurance that the party seeking the information made reasonable efforts to secure a qualified protective order. Among other corrective actions to remedy this situation, OCR required that the hospital revise its subpoena processing procedures. Under the revised process, if a subpoena is received that does not meet the requirements of the Privacy Rule, the information is not disclosed; instead, the hospital contacts the party seeking the subpoena and the requirements of the Privacy Rule are explained. The hospital also trained relevant staff members on the new procedures.

# A HIPAA Compliant Office

- Training of Staff/Faculty/Interns
- Physical Security Measures
- Confidentiality Agreements with all business associates

# Conclusion

# Today's Take-aways

- A HIPAA compliant chiropractic office:
  - Measures in place to protect PHI
  - Encrypted communications
  - Appropriate forms

# Keep in Touch

- Michelle J Massa, DC, CEES
  - www.MichelleJMassa.com
  - Email: michellemassadc@gmail.com
  - Facebook: Michelle Massa
  - Facebook Page: Michelle J Massa, DC, CEES
  - Linked in: Michelle J. Massa https://www.linkedin.com/in/michellejmassadc
  - Instagram: @MichelleJMassa

# Thanks So Much For Being Here Today!


**Hope To See You Soon**

***Back To Chiropractic CE Seminars!***

**backtochiropractic.net**